Draft NIST Special Publication 800-37
Revision 2

Risk Management Framework for Information Systems and Organizations

A System Life Cycle Approach for Security and Privacy

This publication contains comprehensive updates to the *Risk Management Framework*. These updates include an alignment with the constructs in the NIST Cybersecurity Framework; the integration of privacy risk management processes; an alignment with system life cycle security engineering processes; and the incorporation of supply chain risk management processes. Organizations can use the frameworks and processes in a complementary manner within the RMF to effectively manage security and privacy risks to organizational operations and assets, individuals, other organizations, and the Nation. This update includes organization-wide RMF tasks that are designed to prepare information system owners to conduct system-level risk management activities. The intent is to increase the efficiency and effectiveness of the RMF by establishing a closer connection to the organization's missions and business functions and improving the communications among senior leaders, managers, and operational personnel.

JOINT TASK FORCE

FINAL PUBLIC DRAFT

National Institute of
Standards and Technology
U.S. Department of Commerce

Draft NIST Special Publication 800-37
Revision 2

Risk Management Framework for Information Systems and Organizations

A System Life Cycle Approach for Security and Privacy

October 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA), 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of the appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, OMB Director, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-37, Revision 2
Natl. Inst. Stand. Technol. Spec. Publ. 800-37, Rev. 2, **176 pages** (October 2018)

CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts, practices, and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review draft publications during the designated public comment periods and provide feedback to NIST. Many NIST publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Public comment period: October 2 through October 31, 2018

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: sec-cert@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA) [FOIA96].

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) promotes the U.S. economy and public welfare by providing technical leadership for the Nation’s measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology (IT). ITL’s responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL’s research, guidelines, and outreach efforts in information systems security and privacy and its collaborative activities with industry, government, and academic organizations.

Abstract

This publication provides guidelines for applying the Risk Management Framework (RMF) to information systems and organizations. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information system categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. The RMF includes activities to prepare organizations to execute the framework at appropriate risk management levels. The RMF also promotes near real-time risk management and ongoing information system and common control authorization through the implementation of continuous monitoring processes; provides senior leaders and executives with the necessary information to make efficient, cost-effective, risk management decisions about the systems supporting their missions and business functions; and incorporates security and privacy into the system development life cycle. Executing the RMF tasks links essential risk management processes at the system level to risk management processes at the organization level. In addition, it establishes responsibility and accountability for the controls implemented within an organization’s information systems and inherited by those systems.

Keywords

assess; authorization to operate; authorization to use; authorizing official; categorize; common control; common control authorization; common control provider; continuous monitoring; control assessor; control baseline; hybrid control; information owner or steward; monitor; ongoing authorization; plan of action and milestones; privacy; privacy assessment report; privacy control; privacy plan; privacy risk; profile; risk assessment; risk executive function; risk management; risk management framework; security; security assessment report; security control; security plan; security risk; senior agency information security officer; senior agency official for privacy; supply chain risk management; system development life cycle; system owner; system privacy officer; system security officer; system-specific control.

Acknowledgements

This publication was developed by the *Joint Task Force* Interagency Working Group. The group includes representatives from the Civil, Defense, and Intelligence Communities. The National Institute of Standards and Technology wishes to acknowledge and thank the senior leaders from the Departments of Commerce and Defense, the Office of the Director of National Intelligence, the Committee on National Security Systems, and the members of the interagency working group whose dedicated efforts contributed significantly to the publication.

Department of Defense

Dana Deasy
Chief Information Officer

Essye B. Miller
Principal Deputy CIO and DoD Senior Information Security Officer

Thomas P. Michelli
Acting Deputy CIO for Cybersecurity

Vicki Michetti
Director, Cybersecurity Policy, Strategy, International, and Defense Industrial Base Directorate

Office of the Director of National Intelligence

John Sherman
Chief Information Officer

Vacant
Deputy Chief Information Officer

Susan Dorr
Director, Cybersecurity Division and Chief Information Security Officer

Wallace Coggins
Director, Security Coordination Center

National Institute of Standards and Technology

Charles H. Romine
Director, Information Technology Laboratory

Donna Dodson
Cybersecurity Advisor, Information Technology Laboratory

Matt Scholl
Chief, Computer Security Division

Kevin Stine
Chief, Applied Cybersecurity Division

Ron Ross
FISMA Implementation Project Leader

Committee on National Security Systems

Edward Brindley
Chair

Susan Dorr
Co-Chair

Kevin Dulany
Tri-Chair—Defense Community

Peter H. Duspiva
Tri-Chair—Intelligence Community

Vacant
Tri-Chair—Civil Agencies

Joint Task Force Interagency Working Group

Ron Ross *NIST, JTF Leader*	Kevin Dulany *DoD*	Peter Duspiva *Intelligence Community*	Kelley Dempsey *NIST*
Taylor Roberts *OMB*	Ellen Nadeau *NIST*	Victoria Pillitteri *NIST*	Naomi Lefkovitz *NIST*
Jordan Burris *OMB*	Charles Cutshall *OMB*	Kevin Herms *OMB*	Carol Bales *OMB*
Jeff Marron *NIST*	Kaitlin Boeckl *NIST*	Kirsten Moncada *OMB*	Jon Boyens *NIST*
Dorian Pappas *CNSS*	Dominic Cussatt *Veterans Affairs*	Martin Stanley *DHS*	Celia Paulsen *NIST*

The authors also wish to recognize Matt Barrett, Kathleen Coupe, Jeff Eisensmith, Ned Goren, Matthew Halstead, Jody Jacobs, Ralph Jones, Martin Kihiko, Raquel Leone, and the scientists, engineers, and research staff from the Computer Security Division and the Applied Cybersecurity Division for their exceptional contributions in helping to improve the content of the publication. A special note of thanks goes to Jim Foti and Elizabeth Lennon for their excellent technical editing and administrative support.

In addition, the authors wish to acknowledge the United States Air Force and the "RMF Next" initiative, facilitated by Air Force CyberWorx, that provided the inspiration for some of the new ideas in the RMF 2.0. The working group, led by Lauren Knausenberger, Bill Bryant, and Venice Goodwine, included government and industry representatives Jake Ames, Chris Bailey, James Barnett, Steve Bogue, Wes Chiu, Shane Deichman; Joe Erskine, Terence Goodman, Jason Howe, Brandon Howell, Todd Jacobs, Peter Klabe, William Kramer, Bryon Kroger, Dihn Le, Noam Liran, Sam Miles, Michael Morrison, Raymond Tom Nagley, Wendy Nather, Jasmine Neal, Ryan Perry, Eugene Peterson, Lawrence Rampaul, Jessica Rheinschmidt, Greg Roman, Susanna Scarveles, Justin Schoenthal, Christian Sorenson, Stacy Studstill, Charles Wade, Shawn Whitney, David Wilcox, and Thomas Woodring.

Finally, the authors also gratefully acknowledge the significant contributions from individuals and organizations in both the public and private sectors, nationally and internationally, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication.

HISTORICAL CONTRIBUTIONS TO NIST SPECIAL PUBLICATION 800-37

The authors acknowledge the many individuals who contributed to previous versions of Special Publication 800-37 since its inception in 2005. They include Marshall Abrams, William Barker, Beckie Koonge, Roger Caslow, John Gilligan, Peter Gouldmann, Richard Graubart, John Grimes, Gus Guissanie, Priscilla Guthrie, Jennifer Fabius, Cita Furlani, Richard Hale, Peggy Himes, William Hunteman, Arnold Johnson, Donald Jones, Stuart Katzke, Eustace King, Mark Morrison, Sherrill Nicely, Esten Porter, Karen Quigg, George Rogers, Cheryl Roby, Gary Stoneburner, Marianne Swanson, Glenda Turner, and Peter Williams.

Notes to Reviewers

This is the final draft of NIST Special Publication 800-37, Revision 2. We have incorporated changes to the publication in response to the comments received during the initial public comment period. In addition to seeking your comments on those changes, we are also seeking feedback on a new RMF Task P-13, *Information Life Cycle*. The life cycle describes the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion. Identifying and understanding all stages of the information life cycle have significant implications for security and privacy. We are seeking comments on how organizations would execute this task and how we might provide the most helpful discussion to assist organizations in the execution.

Your feedback on this draft publication is important to us. We appreciate each contribution from our reviewers. The very insightful comments from both the public and private sectors, nationally and internationally, continue to help shape the final publication to ensure that it meets the needs and expectations of our customers. NIST anticipates publishing the final version of this publication by **December 2018**.

- **RON ROSS**
  NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Executive Summary

As we push computers to “the edge” building an increasingly complex world of interconnected information systems and devices, security, privacy, and supply chain issues continue to be a large part of the national conversation. The Defense Science Board Report, *Resilient Military Systems and the Advanced Cyber Threat* [DSB 2013], provides a sobering assessment of the vulnerabilities in the United States Government, the U.S. critical infrastructure, and the systems that support the mission-essential operations and assets in the public and private sectors.

> *“…The Task Force notes that the cyber threat to U.S. critical infrastructure is outpacing efforts to reduce pervasive vulnerabilities, so that for the next decade at least the United States must lean significantly on deterrence to address the cyber threat posed by the most capable U.S. adversaries. It is clear that a more proactive and systematic approach to U.S. cyber deterrence is urgently needed…”*

There is an urgent need to further strengthen the underlying information systems, component products, and services that we depend on in every sector of the critical infrastructure—ensuring that those systems, products, and services are sufficiently trustworthy throughout the system development life cycle (SDLC) and can provide the necessary resilience to support the economic and national security interests of the United States. System modernization, the aggressive use of automation, and the consolidation, standardization, and optimization of federal systems and networks to strengthen the protection for high-value assets, are key objectives for the federal government.

Executive Order (E.O.) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* [EO 13800] recognizes the increasing interconnectedness of Federal information systems and requires agency heads to ensure appropriate risk management not only for the Federal agency’s enterprise, but also for the Executive Branch as a whole. The E.O. states:

> *“…The executive branch operates its information technology (IT) on behalf of the American people. Its IT and data should be secured responsibly using all United States Government capabilities...”*

> *“…Cybersecurity risk management comprises the full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents…”*

OMB Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* [OMB M-17-25] provides implementation guidance to Federal agencies for E.O. 13800. The memorandum states:

> *“… An effective enterprise risk management program promotes a common understanding for recognizing and describing potential risks that can impact an agency’s mission and the delivery of services to the public. Such risks include, but are not limited to, strategic, market, cyber, legal, reputational, political, and a broad range of operational risks such as information security, human capital, business continuity, and related risks…”*

> *“… Effective management of cybersecurity risk requires that agencies align information security management processes with strategic, operational, and budgetary planning processes…”*

OMB Circular A-130, *Managing Information as a Strategic Resource* [OMB A-130], addresses responsibilities for protecting federal information resources and for managing personally identifiable information (PII). Circular A-130 requires agencies to implement the RMF that is described in this guideline and requires agencies to integrate privacy into the RMF process. In establishing requirements for information security programs and privacy programs, the OMB circular emphasizes the need for both programs to collaborate on shared objectives:

> *"While security and privacy are independent and separate disciplines, they are closely related, and it is essential for agencies to take a coordinated approach to identifying and managing security and privacy risks and complying with applicable requirements…."*

This update to NIST Special Publication 800-37 (Revision 2) responds to the call by the Defense Science Board, the Executive Order, and the OMB policy memorandum to develop the next-generation Risk Management Framework (RMF) for information systems, organizations, and individuals.

There are seven major objectives for this update:

- To provide closer linkage and communication between the risk management processes and activities at the C-suite or governance level of the organization and the individuals, processes, and activities at the system and operational level of the organization;
- To institutionalize critical risk management preparatory activities at all risk management levels to facilitate a more effective, efficient, and cost-effective execution of the RMF;
- To demonstrate how the NIST Cybersecurity Framework [NIST CSF]can be aligned with the RMF and implemented using established NIST risk management processes;
- To integrate privacy risk management processes into the RMF to better support the privacy protection needs for which privacy programs are responsible;
- To promote the development of trustworthy secure software and systems by aligning life cycle-based systems engineering processes in NIST Special Publication 800-160, Volume 1 [NIST 800-160-1], with the relevant tasks in the RMF;
- To integrate security-related, supply chain risk management (SCRM) concepts into the RMF to address untrustworthy suppliers, insertion of counterfeits, tampering, unauthorized production, theft, insertion of malicious code, and poor manufacturing and development practices throughout the SDLC; and
- To allow for an organization-generated control selection approach to complement the traditional baseline control selection approach and support the use of the consolidated control catalog in NIST Special Publication 800-53, Revision 5.

The addition of the *Prepare* step is one of the key changes to the RMF—incorporated to achieve more effective, efficient, and cost-effective security and privacy risk management processes. The primary objectives for institutionalizing organization-level and system-level preparation are:

- To facilitate effective communication between senior leaders and executives at the organization and mission/business process levels and system owners at the operational level.
- To facilitate organization-wide identification of common controls and the development of organization-wide tailored control baselines, reducing the workload on individual system owners and the cost of system development and asset protection.

- To reduce the complexity of the information technology (IT) and operations technology (OT) infrastructure using Enterprise Architecture concepts and models to consolidate, optimize, and standardize organizational systems, applications, and services.
- To identify, prioritize, and focus resources on the organization's high-value assets (HVA) that require increased levels of protection—taking measures commensurate with the risk to such assets.

By achieving the above objectives, organizations can **simplify** RMF execution, employ **innovative** approaches for managing risk, and increase the level of **automation** when carrying out specific tasks. Organizations implementing "RMF 2.0" will be able to:

- Use the tasks and outputs of the Organization-Level and System-Level *Prepare* step to promote a consistent starting point within organizations to execute the RMF;
- Maximize the use of common controls at the organization level to promote standardized, consistent, and cost-effective security and privacy capability inheritance;
- Maximize the use of shared or cloud-based systems, services, and applications to reduce the number of authorizations needed across the organization;
- Employ organization-wide tailored control baselines to increase the speed of security and privacy plan development and the consistency of security and privacy plan content;
- Employ organization-defined controls based on security and privacy requirements generated from a systems security engineering process;
- Maximize the use of automated tools to manage security categorization; control selection, assessment, and monitoring; and the authorization process;
- Decrease the level of effort and resource expenditures for low-impact systems if those systems cannot adversely affect higher-impact systems through system connections;
- Maximize the reuse of RMF artifacts (e.g., security and privacy assessment results) for standardized hardware/software deployments, including configuration settings;
- Reduce the complexity of the IT/OT infrastructure by eliminating unnecessary systems, system components, and services — employing the least functionality principle;
- Make the transition to ongoing authorization a priority and use continuous monitoring approaches to reduce the cost and increase the efficiency of security and privacy programs.

Recognizing that the preparation for RMF execution may vary from organization to organization, achieving the above objectives can reduce the overall IT/OT footprint and attack surface of organizations, promote IT modernization objectives, conserve resources, prioritize security activities to focus protection strategies on the most critical assets and systems, and promote privacy protections for individuals.

COMMON SECURITY AND PRIVACY RISK FOUNDATIONS

In developing standards and guidelines, NIST consults with federal agencies, state, local, and tribal governments, and private sector organizations; avoids unnecessary and costly duplication of effort; and ensures that its publications are complementary with the standards and guidelines used for the protection of national security systems. In addition to implementing a transparent public review process for its publications, NIST collaborates with the Office of Management and Budget, the Office of the Director of National Intelligence, the Department of Defense, and the Committee on National Security Systems, and has established a unified risk management framework for the federal government. This common foundation provides the Civil, Defense, and Intelligence Communities of the federal government and their contractors, cost-effective, flexible, and consistent methods and techniques to manage security and privacy risks to organizational operations and assets, individuals, other organizations, and the Nation. The unified framework also provides a strong basis for reciprocal acceptance of assessment results and authorization decisions and facilitates information sharing and collaboration. NIST continues to work with public and private sector entities to establish mappings and relationships between its security and privacy standards and guidelines and those developed by external organizations.

276

ACCEPTANCE OF SECURITY AND PRIVACY RISK

The Risk Management Framework addresses security and privacy risk from two perspectives—an information system perspective and a common controls perspective. For an information system, authorizing officials issue an *authorization to operate* or *authorization to use* for the system, accepting the security and privacy risks to the organization's operations and assets, individuals, other organizations, and the Nation. For common controls, authorizing officials issue a *common control authorization* for a specific set of controls that can be inherited by designated organizational systems, accepting the security and privacy risks to the organization's operations and assets, individuals, other organizations, and the Nation. Authorizing officials also consider the risk of inheriting common controls as part of their system authorizations. The different types of authorizations are described in Appendix F.

THE RMF IS TECHNOLOGY NEUTRAL

The RMF is purposefully designed to be technology neutral so that the methodology can be applied to any type of information system* without modification. While the specific controls selected, control implementation details, and control assessment methods and objects may vary with different types of IT resources, there is no need to adjust the RMF process to accommodate specific technologies.

All information systems process, store, or transmit some type of information. For example, information about the temperature in a remote facility collected and transmitted by a sensor to a monitoring station, location coordinates transmitted by radio to a controller on a weapons system, photographic images transmitted by a remote camera (land/satellite-based) to a server, or health IT devices transmitting patient information via a hospital network, require protection. This information can be protected by: categorizing the information to determine the impact of loss; assessing whether the processing of the information could impact individuals' privacy; and selecting and implementing controls that are applicable to the IT resources in use. Therefore, cloud-based systems, industrial/process control systems, weapons systems, cyber physical systems, applications, IoT devices, or mobile devices/systems, do not require a separate risk management process but rather a tailored control set and specific implementation details determined by applying the existing RMF process.

The RMF is applied iteratively, as applicable, during the system development life cycle for any type of system development approach (including *Agile* and *DevOps* approaches). The security and privacy requirements and controls are implemented, verified, and validated as development progresses throughout the life cycle. This flexibility allows the RMF to support rapid technology cycles, innovation, and the use of current best practices in system and system component development.

* **Note:** The publication pertains to information systems, which are discrete sets of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether such information is in digital or non-digital form. Information resources include information and related resources, such as personnel, equipment, funds, and information technology. Therefore, information systems may or may not include hardware, firmware, and software.

278

USE OF AUTOMATION IN THE EXECUTION OF THE RMF

Organizations should maximize the use of *automation*, wherever possible, to increase the speed, effectiveness, and efficiency of executing the steps in the Risk Management Framework (RMF). Automation is particularly useful in the assessment and continuous monitoring of controls, the preparation of authorization packages for timely decision-making, and the implementation of ongoing authorization approaches—together facilitating a real-time or near real-time risk-based decision-making process for senior leaders. Organizations have significant flexibility in deciding when, where, and how to use automation or automated support tools for their security and privacy programs. In some situations, automated assessments and monitoring of controls may not be possible or feasible.

SCOPE AND APPLICABILITY

This publication is intended to help organizations manage security and privacy risk, and to satisfy the requirements in the Federal Information Security Modernization Act of 2014 (FISMA), the Privacy Act of 1974, OMB policies, and Federal Information Processing Standards, among other laws, regulations, and policies. The scope of this publication pertains to federal information systems, which are discrete sets of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether such information is in digital or non-digital form. Information resources include information and related resources, such as personnel, equipment, funds, and information technology.

MANAGING RISK

Using the Cybersecurity Framework

Executive Order (E.O.) 13800 requires federal agencies to modernize their IT infrastructure and systems and recognizes the increasing interconnectedness of federal information systems and networks. The E.O. also requires agency heads to manage risk at the agency level and across the Executive Branch using the *Framework for Improving Critical Infrastructure Cybersecurity* (also known as the Cybersecurity Framework). And finally, the E.O. reinforces the Federal Information Security Modernization Act (FISMA) of 2014 by holding agency heads accountable for managing the cybersecurity risk to their organizations.

The Cybersecurity Framework is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes. Therefore, consistent with OMB Memorandum M-17-25, the federal implementation of the Cybersecurity Framework fully supports the use of and is consistent with the risk management processes and approaches defined in [SP 800-39] and NIST Special Publication 800-37. This allows agencies to meet their concurrent obligations to comply with the requirements of FISMA and E.O. 13800.

Each task in the RMF includes references to specific sections in the Cybersecurity Framework. For example, Task P-2, *Risk Management Strategy*, aligns with the Cybersecurity Framework Core [Identify Function]; Task P-4, *Organization-Wide Tailored Control Baselines and Profiles*, aligns with Cybersecurity Framework Profile construct; and Task R-5, *Authorization Reporting*, and Task M-5, *Posture Reporting*, support OMB reporting and risk management requirements organization-wide by using the Cybersecurity Framework constructs of Functions, Categories, and Subcategories. The subcategory mappings to the [SP 800-53] controls are available at: https://www.nist.gov/cyberframework/federal-resources.

SECURITY AND PRIVACY IN THE RMF

Organizations are encouraged to collaborate on the plans, assessments, and POAMs for security and privacy issues to maximize efficiency and reduce duplication of effort. The objective is to ensure that security and privacy requirements derived from laws, executive orders, directives, regulations, policies, standards, or missions and business functions are adequately addressed, and the appropriate controls are selected, implemented, assessed, and monitored on an ongoing basis. The authorization decision, a key step in the RMF, depends on the development of credible and actionable security and privacy evidence generated for the authorization package. Creating such evidence in a cost-effective and efficient manner is important.

The unified and collaborative approach to bring security and privacy evidence together in a single authorization package will support authorizing officials with critical information from security and privacy professionals to help inform the authorization decision. In the end, it is not about generating additional paperwork, artifacts, or documentation. Rather, it is about ensuring greater visibility into the implementation of security and privacy controls which will promote more informed, risk-based authorization decisions.

Table of Contents

CHAPTER ONE

INTRODUCTION

THE NEED TO MANAGE SECURITY AND PRIVACY RISK

Organizations depend on information systems[1] to carry out their missions and business functions and those systems are constantly subject to serious threats. The threats to information systems include environmental disruptions, human or machine errors, and purposeful attacks that are often disciplined, well-organized, and well-funded. These attacks in many cases are very sophisticated.[2] When successful, attacks on information systems can result in serious or catastrophic damage to organizational operations[3] and assets, individuals, other organizations, and the Nation.[4] Given the significant and ever-increasing danger of those threats, it is imperative that organizations remain vigilant and that executives, leaders, and managers at all organizational levels understand their responsibilities and are accountable for protecting organizational assets and for managing security and privacy risks.[5]

In addition to the responsibility to protect organizational assets from the threats that exist in today's environment, organizations have a responsibility to consider and manage the risks to individuals when information systems process personally identifiable information (PII).[6] [7] The information security and privacy programs implemented by organizations have complementary objectives with respect to managing the confidentiality, integrity, and availability of PII. While many privacy risks arise from unauthorized activities that lead to the loss of confidentiality, integrity, or availability of PII, other privacy risks result from authorized activities involving the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII that enables an organization to meet its mission or business objectives. For example, organizations could fail to provide appropriate notice of PII processing depriving an individual of knowledge of such processing or an individual could be embarrassed or stigmatized by the authorized disclosure of PII. While managing privacy risk requires close coordination

[1] An *information system* is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information [See 44 U.S.C. Sec. 3502]. The term information system includes, for example, general-purpose computing systems; industrial/process control systems; cyber-physical systems; weapons systems; super computers; command, control, and communications systems; devices such as smart phones and tablets; environmental control systems; embedded devices/sensors; and paper-based systems.

[2] Defense Science Board Task Force Report, *Resilient Military Systems and the Advanced Cyber Threat* [DSB 2013].

[3] Organizational operations include mission, functions, image, and reputation.

[4] Adverse impacts include, for example, compromises to systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.

[5] Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event. Risk is also a function of the adverse impacts that arise if the circumstance or event occurs, and the likelihood of occurrence. Types of risk include program risk; compliance/regulatory risk; financial risk; legal risk; mission/business risk; political risk; security risk; privacy risk; project risk; reputational risk; safety risk; strategic planning risk; and supply chain risk.

[6] [OMB A-130] defines PII as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."

[7] Organizations may also choose to consider risks to individuals that may arise from interactions with information systems, where the processing of PII may be less impactful than the effect the system has on individuals' behavior or activities. Such effects would constitute risks to individual autonomy and organizations may need to take steps to manage those risks in addition to information security and privacy risks.

between information security and privacy programs due to the complementary nature of the programs' objectives around the confidentiality, integrity, and availability of PII, privacy risks also raise distinct concerns that require specialized expertise and approaches. Therefore, it is critical that organizations also establish and maintain robust privacy programs to ensure compliance with applicable privacy requirements and to manage the risk to individuals associated with the processing of PII.

In addition to information security and privacy risks, supply chain risk[8] is also of growing concern to organizations. Because of the increased reliance on third-party or external providers and commercial-off-the-shelf products, systems, and services, attacks or disruptions in the supply chain which impact an organization's systems are increasing. Such attacks can be difficult to trace or manage and can result in serious, severe, or catastrophic, long-standing consequences for an organization's systems. Supply chain risk management (SCRM) overlaps and works in harmony with security and privacy risk management. For this publication, it is integrated in to security, but also specially called out in several areas to add emphasis and clarification, and to help promote a comprehensive security and privacy risk management approach.

1.1 BACKGROUND

NIST in its partnership with the Department of Defense, the Office of the Director of National Intelligence, and the Committee on National Security Systems, developed a *Risk Management Framework* (RMF) to improve information security, strengthen risk management processes, and encourage reciprocity[9] among organizations. In July 2016, the Office of Management and Budget (OMB) revised Circular A-130 to include responsibilities for privacy programs under the RMF.

The RMF emphasizes risk management by promoting the development of security and privacy capabilities into information systems throughout the system development life cycle (SDLC);[10] by maintaining situational awareness of the security and privacy posture of those systems on an ongoing basis through continuous monitoring processes; and by providing information to senior leaders and executives to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the use and operation of their systems. The RMF:

- Provides a repeatable process designed to promote the protection of information and information systems commensurate with risk;
- Emphasizes organization-wide preparation necessary to manage security and privacy risks;
- Facilitates the categorization of information and systems, the selection, implementation, assessment, and monitoring of controls, and the authorization of information systems and common controls;
- Promotes the use of automation for near real-time risk management and ongoing system and control authorization through the implementation of continuous monitoring processes;

[8] SCRM requirements are promulgated in [OMB A-130], [DODI 5200.44], and for National Security Systems in [CNSSD 505]. SCRM requirements have also been addressed by the Federal SCRM Policy Coordinating Committee.

[9] *Reciprocity* is a mutual agreement among participating organizations to accept each other's security assessment results to reuse system resources and/or to accept each other's assessed security posture to share information.

[10] [SP 800-64] provides guidance on security considerations in the SDLC.

- Encourages the use of correct and timely metrics to provide senior leaders and managers with the necessary information to make cost-effective, risk-based decisions for information systems supporting their missions and business functions;
- Facilitates the integration of security and privacy requirements and controls into enterprise architecture,[11] SDLC, acquisition processes, and systems engineering processes;
- Connects risk management processes at the organization and mission/business process levels to risk management processes at the information system level through a senior accountable official for risk management and risk executive (function);[12] and
- Establishes responsibility and accountability for controls implemented within information systems and inherited by those systems.

The RMF provides a dynamic and flexible approach to effectively manage security and privacy risks in diverse environments with complex and sophisticated threats, evolving missions and business functions, and changing system and organizational vulnerabilities. The framework is policy and technology neutral which facilitates ongoing upgrades to IT resources[13] and IT modernization efforts to support and help ensure critical missions and essential services during such transition periods.

1.2 PURPOSE AND APPLICABILITY

This publication provides guidelines for applying the RMF to information systems and organizations. The guidelines have been developed:

- To ensure that managing system-related security and privacy risk is consistent with the mission and business objectives of the organization and risk management strategy established by the senior leadership through the risk executive (function);
- To achieve privacy protections for individuals and security protections for information and information systems through the implementation of appropriate risk response strategies;
- To facilitate the implementation of the *Framework for Improving Critical Infrastructure Cybersecurity* [NIST CSF] within federal organizations.[14]
- To facilitate the integration of security and privacy requirements and controls into enterprise architecture, SDLC processes, acquisition processes, and systems engineering processes;[15] and
- To support consistent, informed, and ongoing authorization decisions (through continuous monitoring),[16] reciprocity, and the transparency and traceability of security and privacy information.

[11] [OMB FEA] provides guidance on the Federal Enterprise Architecture.

[12] [OMB M-17-25] provides guidance on risk management roles and responsibilities.

[13] IT resources refer to the information technology component of *information resources* defined in [OMB A-130].

[14] [EO 13800] directs federal agencies to use the [NIST CSF] to manage cybersecurity risk.

[15] [SP 800-160-1] provides guidance on systems security engineering and building trustworthy, secure systems.

[16] [SP 800-137] provides guidance on information security continuous monitoring. Future updates to this publication will also address privacy continuous monitoring.

This publication is intended to help organizations manage security and privacy risk and to satisfy the security and privacy requirements in the Federal Information Security Modernization Act of 2014 [FISMA14], the Privacy Act of 1974 [PRIV74], OMB policies (e.g., [OMB A-130]), and designated Federal Information Processing Standards, among other laws, regulations, and policies.

The scope of this publication pertains to federal information systems, which are discrete sets of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether such information is in digital or non-digital form. Information resources include information and related resources, such as personnel, equipment, funds, and information technology. The guidelines have been developed from a technical perspective to complement guidelines for national security systems and may be used for such systems with the approval of appropriate federal officials with policy authority over such systems. State, local, and tribal governments, as well as private sector organizations are encouraged to use these guidelines, as appropriate.

1.3 TARGET AUDIENCE

This publication serves individuals associated with the design, development, implementation, assessment, operation, maintenance, and disposition of information systems including:

- Individuals with mission or business ownership responsibilities or fiduciary responsibilities including, for example, and heads of federal agencies;
- Individuals with information system development and acquisition responsibilities, including, for example, program managers, procurement officials, component product and system developers, systems integrators, and enterprise architects;
- Individuals with logistical or disposition-related responsibilities, including, for example, program managers, procurement officials, system integrators, and property managers;
- Individuals with information system, information security, or privacy management, oversight, or governance responsibilities including, for example, senior leaders, risk executives, authorizing officials, chief information officers, senior agency information security officers, and senior agency officials for privacy;
- Individuals responsible for conducting security or privacy assessments and for monitoring information systems, for example, control assessors, auditors, and system owners; and
- Individuals with security or privacy implementation and operational responsibilities, for example, system owners, common control providers, information owners/stewards, mission or business owners, security or privacy architects, and systems security or privacy engineers.

1.4 ORGANIZATION OF THIS PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the concepts associated with managing information system-related security and privacy risk. This includes an organization-wide view of risk management; the RMF steps and structure; the relationship between security and privacy and how both are used in the RMF; system and system elements; authorization boundaries; the allocation of controls to systems and organizations; security and privacy posture; and considerations related to supply chain risk management.

- **Chapter Three** describes the tasks required to implement the steps in the RMF including: organization-level and information system-level preparation; categorization of information and information systems; control selection, tailoring, and implementation; assessment of control effectiveness; information system and common control authorization; the ongoing monitoring of controls; and maintaining awareness of the security and privacy posture of information systems and the organization.

- **Supporting Appendices** provide additional information and guidance for the application of the RMF including: references; glossary of terms; acronyms; roles and responsibilities; summary of tasks; information system and common control authorizations; authorization boundary considerations; and SDLC considerations.

CHAPTER TWO

THE FUNDAMENTALS

HOW TO MANAGE SECURITY AND PRIVACY RISK

This chapter describes the basic concepts associated with managing information system-related security and privacy risk in organizations. These concepts include the RMF steps and task structure; information security and privacy in the RMF; the information system, system elements, and how authorization boundaries are established; control allocations to systems, system elements, and organizations; security and privacy posture; and security and privacy risk management practices associated with the supply chain.

2.1 ORGANIZATION-WIDE RISK MANAGEMENT

Managing information system-related security and privacy risk is a complex undertaking that requires the involvement of the entire organization—from senior leaders providing the strategic vision and top-level goals and objectives for the organization, to mid-level leaders planning, executing, and managing projects, to individuals developing, implementing, operating, and maintaining the systems supporting the organization's missions and business functions. Risk management is a holistic activity that affects every aspect of the organization including the mission and business planning activities, the enterprise architecture, the SDLC processes, and the systems engineering activities that are integral to those system life cycle processes. Figure 1 illustrates a multi-level approach to risk management described in [SP 800-39] that addresses security and privacy risk at the *organization* level, the *mission/business process* level, and the *information system* level. Communication and reporting are bi-directional information flows across the three levels to ensure that risk is addressed throughout the organization.

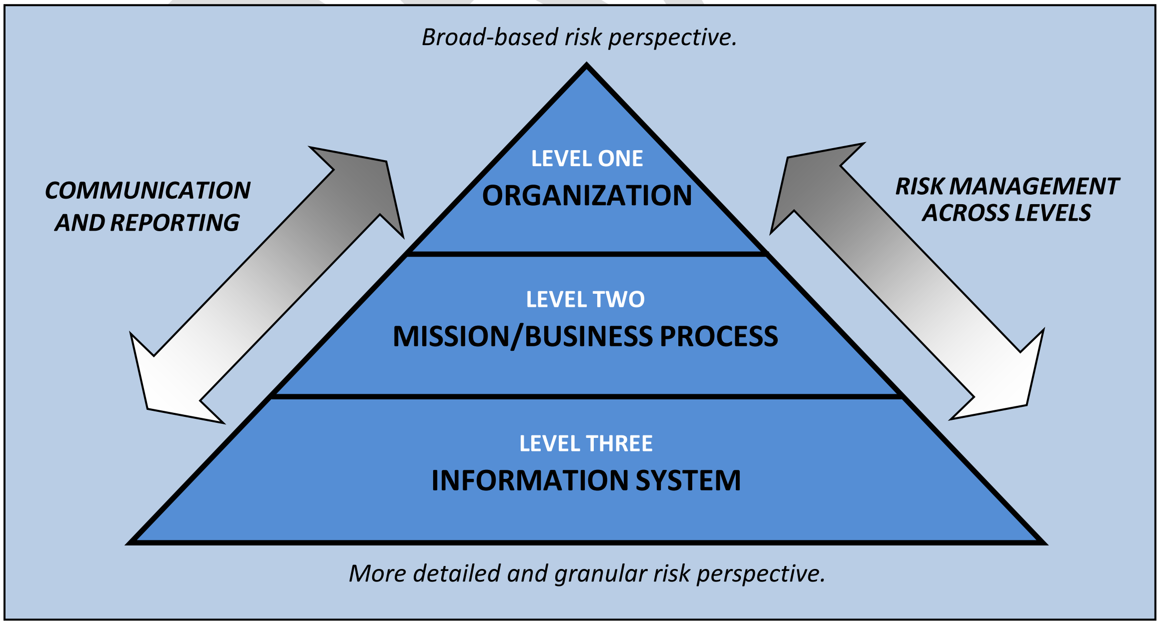

Broad-based risk perspective.
LEVEL ONE
ORGANIZATION
LEVEL TWO
MISSION/BUSINESS PROCESS
LEVEL THREE
INFORMATION SYSTEM
COMMUNICATION AND REPORTING
RISK MANAGEMENT ACROSS LEVELS
More detailed and granular risk perspective.

FIGURE 1: ORGANIZATION-WIDE RISK MANAGEMENT APPROACH

The activities conducted at Levels 1 and 2 are critical to preparing the organization to execute the RMF. Such preparation involves a wide range of activities that go beyond simply managing the security and privacy risk associated with operating or using specific systems and includes activities that are essential to managing security and privacy risk appropriately throughout the organization. Decisions about how to manage such risk at the system level cannot be made in isolation. Such decisions are closely linked to the:

- Mission or business objectives of organizations;
- Modernization initiatives for systems, components, and services;
- Enterprise architecture and the need to manage and reduce the complexity[17] of systems through consolidation, optimization, and standardization;[18] and
- Allocation of resources to ensure the organization can conduct its missions and business operations effectively, efficiently, and in a cost-effective manner.

Preparing the organization to execute the RMF can include:

- Assigning roles and responsibilities for organizational risk management processes;
- Establishing a risk management strategy and organizational risk tolerance;
- Identifying the missions, business functions, and mission/business processes the information system is intended to support;
- Identifying key stakeholders (internal and external to the organization) that have an interest in the information system;
- Identifying and prioritizing assets (including information assets);
- Understanding threats to information systems and organizations;
- Understanding the potential adverse effects on individuals;
- Conducting organization- and system-level risk assessments;
- Identifying and prioritizing security and privacy requirements;[19]
- Determining authorization boundaries for information systems and common controls;[20]
- Defining information systems in terms of the enterprise architecture;
- Developing the security and privacy architectures that include controls suitable for inheritance by information systems;

[17] Managing complexity of systems through consolidation, optimization, and standardization reduces the attack surface and technology footprint exploitable by adversaries.

[18] *Enterprise architecture* defines the mission, information, and the technologies necessary to perform the mission, and transitional processes for implementing new technologies in response to changing mission needs. It also includes a baseline architecture, a target architecture, and a sequencing plan. [OMB FEA] provides guidance for implementing enterprise architectures.

[19] Security and privacy requirements can be obtained from a variety of sources including, for example, laws, executive orders, directives, regulations, policies, standards, and mission/business/operational requirements.

[20] Authorization boundaries determine the scope of authorizations for information systems and common controls (i.e., the system elements that define the system or the set of common controls available for inheritance).

- Identifying, aligning, and deconflicting security and privacy requirements; and
- Allocating security and privacy requirements to information systems, system elements, and organizations.

In contrast to the Level 1 and 2 activities that prepare the organization for the execution of the RMF, Level 3 addresses risk from an *information system* perspective and is guided and informed by the risk decisions at the organization and mission/business process levels. The risk decisions at Levels 1 and 2 can impact the selection and implementation of controls at the system level. Security and privacy requirements are satisfied by the selection and implementation of controls from [SP 800-53]. These controls are allocated to the system as system-specific, hybrid, or common (inherited) controls in accordance with the enterprise architecture, security or privacy architecture, and any tailored control baselines or overlays that have been developed by the organization.[21]

Organizations establish *traceability* of the controls to the security and privacy requirements that the controls are intended to satisfy. Establishing such traceability ensures that all requirements are addressed during system design, development, implementation, operations, maintenance, and disposition.[22] Each level of the risk management hierarchy is a beneficiary of a successful RMF execution—reinforcing the iterative nature of the risk management process where security and privacy risks are framed, assessed, responded to, and monitored at various levels of an organization.

Without adequate risk management preparation at the organizational level, security and privacy activities can become too costly, demand too many skilled security and privacy professionals, and produce ineffective solutions. For example, organizations that fail to define and implement an effective enterprise architecture approach will have difficulty in consolidating, optimizing, and standardizing their information technology infrastructures. Additionally, the effect of architectural and design decisions can adversely affect the ability of organizations to implement effective security and privacy solutions. A lack of adequate preparation by organizations could result in unnecessary redundancy as well as inefficient, costly and vulnerable systems, services, and applications.

2.2 RISK MANAGEMENT FRAMEWORK STEPS AND STRUCTURE

There are seven steps in the RMF; a preparatory step to ensure that organizations are ready to execute the process and six main steps. All seven steps are essential for the successful execution of the RMF. The steps are:

- **Prepare** to execute the RMF from an organization- and a system-level perspective by establishing a context and priorities for managing security and privacy risk.
- **Categorize** the system and the information processed, stored, and transmitted by the system based on a security impact analysis.

[21] Controls can be allocated at all three levels in the risk management hierarchy. For example, common controls may be allocated at the organization, mission/business process, or information system level.

[22] [SP 800-160-1] provides guidance on requirements engineering and traceability.

- **Select** an initial set of controls for the system and tailor the controls as needed to mitigate risk based on an organizational assessment of risk and local conditions.
- **Implement** the controls and describe how the controls are employed within the system and its environment of operation.
- **Assess** the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.
- **Authorize** the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.
- **Monitor** the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

Figure 2 illustrates the steps in the RMF. The RMF operates at all levels in the risk management hierarchy illustrated in Figure 1. Chapter Three provides a detailed description of each of the tasks necessary to carry out the steps in the RMF.

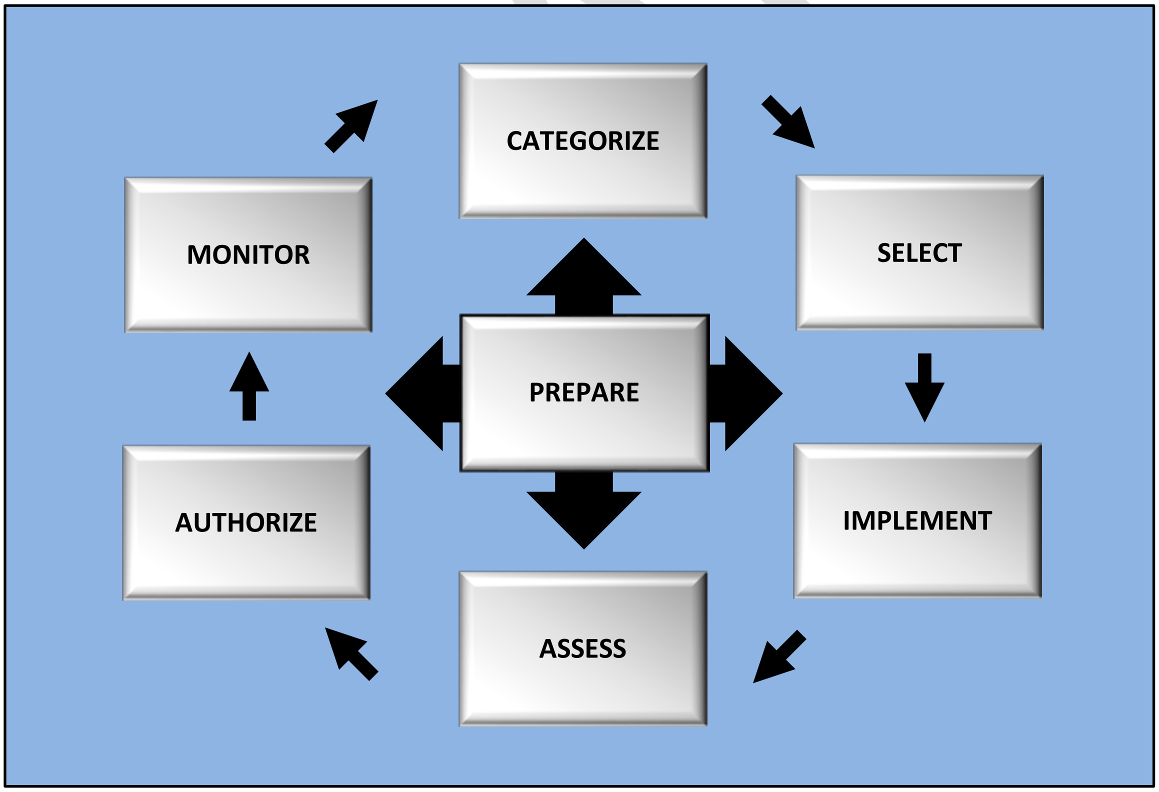


FIGURE 2: RISK MANAGEMENT FRAMEWORK

While the RMF steps are listed in sequential order above and in Chapter Three, the steps following the *Prepare* step can be carried out in a nonsequential order. After completing the tasks in the *Prepare* step, organizations executing the RMF for the first time for a particular system or set of common controls typically carry out the remaining steps in sequential order. However, there could be many points in the risk management process where there is a need to diverge from the sequential order due to the type of system, risk decisions made by senior leadership, or to allow for iterative cycles between tasks or revisiting of tasks (e.g., during agile development). Once the system is in the operations and maintenance phase of the SDLC in the *Continuous Monitoring* step, events may dictate nonsequential execution of steps. For example, changes in risk or in system functionality may necessitate revisiting one or more of the steps in the RMF to address the change.

FLEXIBILITY IN RMF IMPLEMENTATION

Organizations have significant flexibility in executing the steps and tasks of the RMF—including the *selection* of controls and *tailoring* the controls to meet organizational security and privacy needs. The implementation of common controls and control tailoring helps ensure that security and privacy solutions are customized for the missions, business functions, and operating environments of the organization.

Although the risk management approach in Figure 1 is conveyed as hierarchical, project and organization dynamics are typically more complex. The risk management approach selected by an organization may vary on a continuum from top-down command to decentralized consensus among peers. However, in all cases, organizations use a consistent approach that is applied to risk management processes across the enterprise from the *organization* level to the *information system* level. Organizational officials identify and secure the needed resources to complete the risk management tasks described in this publication and ensure that those resources are made available to the appropriate personnel. Resource allocation includes funding to conduct risk management tasks and assigning qualified personnel that will be needed to accomplish the tasks.

Each step in the RMF has a *purpose* statement, a defined set of *outcomes*, and a set of *tasks* that are carried out to achieve those outcomes.[23] Each task contains a set of potential inputs needed to execute the task and a set of potential outputs generated from task execution.[24] In addition, each task describes the risk management roles and responsibilities associated with the task and the phase of the SDLC where task execution occurs.[25] A discussion section provides information related to the task to facilitate understanding and to promote effective task execution. Finally, completing the RMF task description, there is a list of references to provide organizations with supplemental information for each task. Where applicable, the references also identify systems security engineering tasks that correlate with the RMF task.[26]

[23] The outcomes described in this publication can be achieved by different organizational levels—that is, some of the outcomes are universal to the entire organization, while others are system-focused or mission/business unit-focused.

[24] The *potential inputs* for a task may not always be derived from the *potential outputs* from the previous task. This can occur because the RMF steps are not always executed in sequential order, breaking the sequential dependencies.

[25] Appendix D provides a description of each of the roles and responsibilities identified in the tasks.

[26] [SP 800-160-1] describes life cycle-based systems security engineering processes.

The following example illustrates the structure of a typical RMF task:

PLAN REVIEW AND APPROVAL

Task Abbreviation
Select Step Task 6

TASK S-6 Review and approve the security and privacy plans for the system and the environment of operation.

Potential Inputs: Completed security and privacy plans; organization- and system-level risk assessment results.

Potential Outputs: Security and privacy plans approved by the authorizing official.

Primary Responsibility: Authorizing Official or Authorizing Official Designated Representative.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; Chief Acquisition Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

System Development Life Cycle Phase: New – Development/Acquisition.
Existing – Operations/Maintenance.

Explanatory information to facilitate understanding

Discussion: The security and privacy plan review by the authorizing official or designated representative with support from the senior accountable official for risk management or risk executive (function), chief information officer, senior agency information security officer, and senior agency official for privacy, determines if the plans are complete, consistent, and satisfy the stated security and privacy requirements for the system. Based on the results from this review, the authorizing official or designated representative may recommend changes to the security and privacy plans. If the plans are unacceptable, the system owner or common control provider make appropriate changes to the plans. If the plans are acceptable, the authorizing official or designated representative approves the plans.

The acceptance of the security and privacy plans represents an important milestone in the SDLC and risk management process. The authorizing official or designated representative, by approving the plans, agrees to the set of controls (i.e., system-specific, hybrid, or common controls) and the description of the proposed implementation of the controls to meet the security and privacy requirements for the system and the environment in which the system operates. The approval of the plans allows the risk management process to proceed to the RMF *Implement* step. The approval of the plans also establishes the level of effort required to successfully complete the remainder of the RMF steps and provides the basis of the security and privacy specifications for the acquisition of the system or individual system components.

References: [SP 800-30]; [SP 800-53]; [SP 800-160-1] (System Requirements Definition, Architecture Definition, and Design Definition Processes).

2.3 INFORMATION SECURITY AND PRIVACY IN THE RMF

OMB CIRCULAR A-130: INTEGRATION OF INFORMATION SECURITY AND PRIVACY

In 2016, OMB revised Circular A-130, the circular establishing general policy for the planning, budgeting, governance, acquisition, and management of federal information, personnel, equipment, funds, information technology resources, and supporting infrastructure and services. The circular addresses responsibilities for protecting federal information resources and managing personally identifiable information (PII). In establishing requirements for information security programs and privacy programs, the circular emphasizes the need for both programs to collaborate on shared objectives:

> *While security and privacy are independent and separate disciplines, they are closely related, and it is essential for agencies to take a coordinated approach to identifying and managing security and privacy risks and complying with applicable requirements.*

[OMB A-130] requires organizations to implement the RMF that is described in this guideline. With the 2016 revision to the circular, OMB also requires organizations to integrate privacy into the RMF process:

> *The RMF provides a disciplined and structured process that integrates information security, privacy, and risk management activities into the SDLC. This Circular requires organizations to use the RMF to manage privacy risks beyond those that are typically included under the "confidentiality" objective of the term "information security." While many privacy risks relate to the unauthorized access or disclosure of PII, privacy risks may also result from other activities, including the creation, collection, use, and retention of PII; the inadequate quality or integrity of PII; and the lack of appropriate notice, transparency, or participation.*

This section of the guideline describes the *relationship* between information security programs and privacy programs under the RMF. However, subject to OMB policy, organizations retain the flexibility to undertake the integration of privacy into the RMF in the most effective manner, considering the organization's mission and circumstances.

Executing the RMF requires close collaboration between information security programs and privacy programs. While information security programs and privacy programs have different objectives, those objectives are overlapping and complementary. Information security programs are responsible for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction (i.e., unauthorized system activity or behavior) in order to provide confidentiality, integrity, and availability. Privacy programs are responsible for ensuring compliance with applicable privacy requirements and for managing the risks to individuals associated with the creation, collection, use, processing, dissemination, storage, maintenance, disclosure, or disposal (collectively referred to as "processing") of PII.[27] When preparing to execute the steps of the RMF, organizations consider how to best promote and institutionalize collaboration between the two programs to ensure that the objectives of both disciplines are met at every step of the process.

[27] Privacy programs may also choose to consider the risks to individuals that may arise from their interactions with information systems, where the processing of PII may be less impactful than the effect the system has on individuals' behavior or activities. Such effects would constitute risks to individual autonomy and organizations may need to take steps to manage those risks in addition to information security and privacy risks.

When an information system processes PII, the organizations' information security program and privacy program have a shared responsibility for managing the risks to individuals that may arise from unauthorized system activity or behavior. This requires the two programs to collaborate when selecting, implementing, assessing, and monitoring security controls.[28] However, while information security programs and privacy programs have complementary objectives with respect to managing the confidentiality, integrity, and availability of PII, protecting individuals' privacy cannot be achieved solely by securing PII.

Not all privacy risks arise from unauthorized system activity or behavior, such as unauthorized access or disclosure of PII. Some privacy risks may result from authorized activity that is beyond the scope of information security. For example, privacy programs are responsible for managing the risks to individuals that may result from the creation, collection, use, and retention of PII; the inadequate quality or integrity of PII; and the lack of appropriate notice, transparency, or participation. Therefore, to help ensure compliance with applicable privacy requirements and to manage privacy risks from authorized and unauthorized processing of PII, organizations' privacy programs also select, implement, assess, and monitor privacy controls.[29]

[OMB A-130] defines a *privacy control* as an administrative, technical, or physical safeguard employed within an agency to ensure compliance with applicable privacy requirements and to manage privacy risks. A privacy control is different from a *security control*, which the Circular defines as a safeguard or countermeasure prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information. Due to the shared responsibility that organizations' information security programs and privacy programs have to manage the risks to individuals arising from unauthorized system activity or behavior, controls that achieve both security and privacy objectives are both privacy and security controls. This guideline refers to such controls that achieve both sets of objectives simply as "controls." When this guideline uses the descriptors "privacy" and "security" with the term *control*, it is referring to those controls in circumstances where the controls are selected, implemented, and assessed for particular objectives.

The risk management processes described in this publication are equally applicable to security and privacy programs. However, the risks that security and privacy programs are required to manage are overlapping in some areas, but not in others. Consequently, it is important that organizations understand the interplay between privacy and security in order to promote effective collaboration between privacy and security officials at every level of the organization.

[28] For example, in Task C-1 of the *Categorize* step, privacy and security programs work together to consider potential adverse impacts to organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the loss of confidentiality, integrity, or availability of PII in order to determine the impact level for the information system. The resulting impact level drives the selection of a security control baseline in Task S-2 of the *Select* step.

[29] Different controls may need to be selected to mitigate the privacy risks associated with authorized processing of PII. For example, there may be a risk that individuals would be embarrassed or stigmatized if certain information is disclosed about them. While encryption could prevent unauthorized disclosure of PII, it would not address any privacy risks related to disclosures to parties that are authorized to decrypt and access the PII. In order to mitigate this privacy risk, organizations would need to assess the risk of allowing authorized parties to decrypt the information and potentially select controls that would mitigate that risk. In such an example, an organization might select controls to enable individuals to understand the organization's disclosure practices and exercise choices about this access, or use differential privacy or privacy-enhancing cryptographic techniques to disassociate the information from an individual.

2.4 SYSTEM AND SYSTEM ELEMENTS

This publication uses the statutory definition of information system for RMF execution. However, it is important to describe information systems in the context of the SDLC and how security and privacy capabilities are implemented within the components of those systems. Therefore, organizations executing the RMF take a broad view of the life cycle of information system development to provide a contextual relationship and linkage to architectural and engineering concepts that allow security, privacy, and supply chain issues to be addressed throughout the life cycle and at the appropriate level of detail to help ensure that such capabilities are achieved. [ISO 15288] provides an architectural and engineering view of an information system and the entities with which the system interacts in its environment of operation.[30]

Similar to how federal law defines information system as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [ISO 15288] defines a *system* as a set of interacting elements that are organized to achieve one or more stated purposes. Just as the information resources that comprise an information system include information and other resources (e.g., personnel, equipment, funds, and information technology), system elements include technology or machine elements, human elements, and physical or environmental elements. Each of the *system elements*[31] within the system fulfills specified requirements and may be implemented via hardware, software, or firmware;[32] physical structures or devices; or people, processes, policies, and procedures. Individual system elements or a combination of system elements may satisfy stated system requirements. Interconnections between system elements allow those elements to interact as necessary to produce a capability as specified by the system requirements. Finally, every system operates within an environment that influences the system and its operation.

The authorization boundary defines the system[33] for the purpose of RMF execution. The system may be supported by one or more *enabling systems* that provide support during the system life cycle. Enabling systems are not contained within the authorization boundary of the system and do not necessarily exist in the system's environment of operation. An enabling system may provide common (i.e., inherited) controls for the system or may include any type of service or functionality used by the system such as identification and authentication services, network services, or monitoring functionality. Finally, there are *other systems* the system interacts with in the operational environment. These systems are outside of the authorization boundary and may be the beneficiaries of services provided by the system or may simply have some general interaction.

[30] [ISO 15288] is not publicly available. [SP 800-160-1] addresses system security engineering as part of the SDLC.

[31] The terms *system element* and *information resource* are used interchangeably in this publication. Information resources as defined in 44 U.S.C. Sec. 3502 include information and related resources, such as personnel, equipment, funds, and information technology. By law, a system is composed of a discrete set of information resources.

[32] The term *system component* refers to a *system element* that is implemented via hardware, software, or firmware.

[33] Historically, NIST has used the terms *authorization boundary* and *system boundary* interchangeably. In the interest of clarity, accuracy, and use of standardized terminology, the term authorization boundary is now used exclusively to refer to the set of system elements comprising the system to be authorized for operation or authorized for use by an authorizing official (i.e., the scope of the authorization). Authorization boundary can also refer to the set of common controls to be authorized for inheritance purposes.

Figure 3 illustrates the conceptual view of the system and the relationships among the system, system elements, enabling systems, other systems, and the environment of operation.[34]

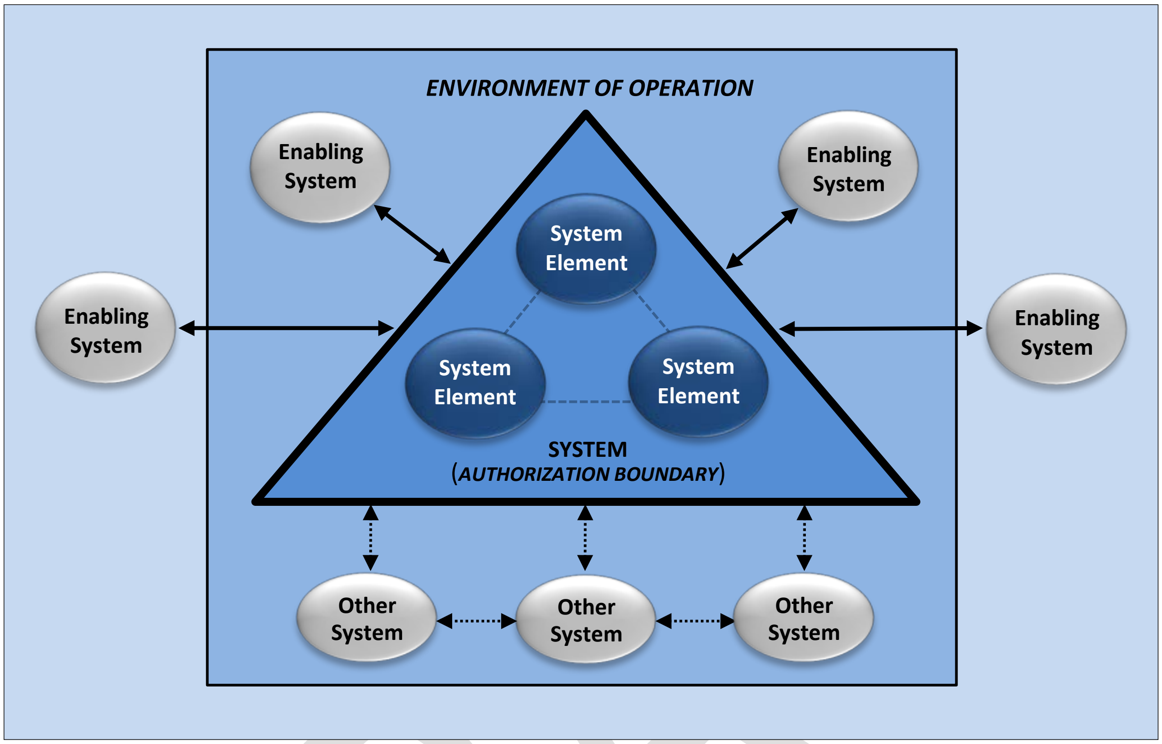


FIGURE 3: CONCEPTUAL VIEW OF THE SYSTEM

As shown in Figure 3, certain parts of the environment of operation for the system are included in the authorization boundary (i.e., determined to be “in scope” for the authorization) while other parts are excluded. For example, the facility that provides protection for a system is part of the environment in which the system operates. As such, the physical and environmental protection controls (e.g., physical access controls at entry points, exterior perimeter protection devices) are included in the security plan for the system and therefore, are included in the authorization boundary.

Conversely, the system may communicate or have other interactions with enabling systems and other systems that are part of the extended environment of operation but are outside of the scope of authorization for the system. Organizations determine which parts of the environment of operation are within the authorization boundary. These determinations are typically specific to the system and are context-driven.

2.5 AUTHORIZATION BOUNDARIES

The authorization boundary establishes the scope of protection for an information system (i.e., what the organization agrees to protect under its direct management or within the scope of its

[34] The terms *system*, *system element*, *enabling system*, *other systems*, and the *environment of operation* are agnostic with respect to information technology (IT) and operations technology (OT).

responsibilities).[35] The authorization boundary includes the people, processes, and information technologies (i.e., system elements) that are part of each system supporting the organization's missions and business functions. Authorization boundaries that are too expansive (i.e., include too many system elements or components) make the risk management process unnecessarily complex. Conversely, authorization boundaries that are too limited (i.e., include too few system elements or components) increase the number of systems that must be separately managed and therefore, may unnecessarily inflate the information security and privacy costs for the organization.

The authorization boundary for a system is established during the RMF *Prepare Task – System level*, Task P-11. Organizations have flexibility in determining what constitutes the authorization boundary for a system. The set of system elements included within an authorization boundary defines the system (i.e., the scope of the authorization). When a set of system elements is identified as an authorization boundary for a system, the elements are generally under the same direct management.[36] Other considerations for determining the authorization boundary include identifying system elements that:

- Support the same mission or business functions;
- Have similar operating characteristics and security and privacy requirements;
- Process, store, and transmit similar types of information (e.g., categorized at the same impact level);[37] or
- Reside in the same environment of operation (or in the case of a distributed system, reside in various locations with similar operating environments).

The scope of the authorization boundary is revisited periodically as part of the continuous monitoring process carried out by the organization. While the above considerations may be useful to organizations in determining authorization boundaries for purposes of managing risk, the considerations are not intended to limit the organization's flexibility in establishing authorization boundaries that promote effective security and privacy with the available resources of the organization.

The process of establishing authorization boundaries carries significant risk management implications and is therefore an organization-wide activity that requires coordination among key participants. The process considers mission and business requirements, security and privacy requirements, and the costs to the organization. Appendix G provides additional information and considerations for determining authorization boundaries, including boundaries for complex systems and software applications.

[35] Information systems are discrete sets of information resources organized for the collection, processing, use, sharing, maintenance, dissemination, or disposition of information, whether such information is in digital or non-digital form. Information resources include information and related resources, such as personnel, equipment, funds, and information technology. Therefore, information systems may or may not include hardware, firmware, and software.

[36] For information systems, direct management control involves budgetary, programmatic, or operational authority and associated *responsibility* and *accountability*. Direct management control does not necessarily imply that there is no intervening management.

[37] If a system contains information at multiple impact levels, the system is categorized at the highest impact level. See [FIPS 199] and [FIPS 200].

EFFECTIVE AUTHORIZATION BOUNDARIES

Establishing effective authorization boundaries for *systems* and *common controls* is one of the most important risk management activities carried out by the organization. The authorization boundary defines the scope of an authorizing official's responsibility for protecting information resources and individuals' privacy.

2.6 CONTROL ALLOCATION

There are three types of controls that can be selected and implemented by organizations: system-specific controls (i.e., controls that provide a security or privacy capability for an information system); common controls (i.e., controls that provide a security or privacy capability for multiple systems); or hybrid controls (i.e., controls that have system-specific and common characteristics). Controls are *allocated* to a system or an organization consistent with the organization's enterprise architecture and security or privacy architecture.[38] This activity is carried out as an organization-wide activity that involves authorizing officials, system owners, common control providers, the chief information officer, the senior accountable official for risk management or risk executive (function); the senior agency information security officer, the senior agency official for privacy, system security or privacy officers, the enterprise architect, and security and privacy architects.[39]

Organizations are encouraged to identify and implement common controls that can support multiple information systems efficiently and effectively as a common protection capability. When these common controls are used to support a specific system, they are referenced by that system as *inherited controls*. Common controls promote cost-effective, efficient, and consistent security and privacy safeguards across the organization and can also simplify risk management processes and activities. By allocating controls to a system as system-specific controls, hybrid controls, or common controls, organizations assign responsibility and accountability to specific organizational entities for the development, implementation, assessment, authorization, and monitoring of those controls. Organizations have significant flexibility in deciding which controls from [SP 800-53] are appropriate for specific types of allocations.

Controls may also be allocated to specific elements within a system. While the control selection process is conducted primarily at the system level, it may not always be necessary to allocate every control in the tailored baseline to each system element. Organizations can save resources by allocating controls to only those system elements that require such protection or that provide such protection for the system.

[38] *Allocation* is the process an organization employs to determine whether controls are system-specific, shared, or common and to assign the controls to the specific system elements (i.e., machine, physical, or human components) responsible for providing a security or privacy capability.

[39] Security control allocation also occurs during the SDLC process as part of *requirements engineering*. [SP 800-160-1] describes the systems security engineering activities associated with system life cycle processes that are needed to achieve trustworthy, secure components, systems, and services.

Figure 4 illustrates control allocation using the RMF to produce risk-related information for the senior leaders and executives (including authorizing officials) in the organization on the security and privacy posture of organizational systems and the mission/business processes supported by those systems.[40]

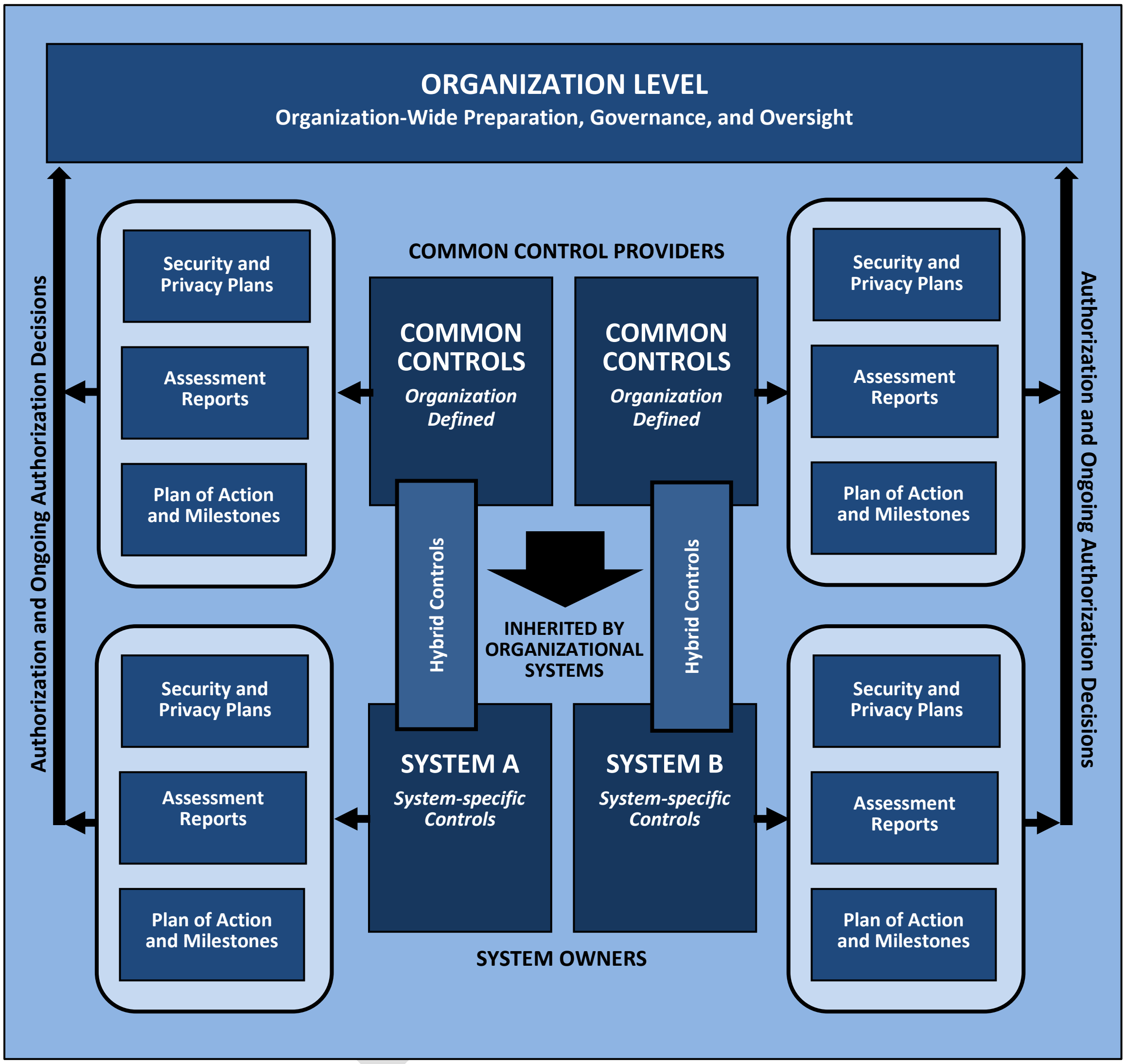

ORGANIZATION LEVEL
Organization-Wide Preparation, Governance, and Oversight
Authorization and Ongoing Authorization Decisions
Security and Privacy Plans
Assessment Reports
Plan of Action and Milestones
COMMON CONTROL PROVIDERS
COMMON CONTROLS
Organization Defined
COMMON CONTROLS
Organization Defined
Security and Privacy Plans
Assessment Reports
Plan of Action and Milestones
Authorization and Ongoing Authorization Decisions
Hybrid Controls
INHERITED BY ORGANIZATIONAL SYSTEMS
Hybrid Controls
Security and Privacy Plans
Assessment Reports
Plan of Action and Milestones
SYSTEM A
System-specific Controls
SYSTEM B
System-specific Controls
SYSTEM OWNERS
Security and Privacy Plans
Assessment Reports
Plan of Action and Milestones

FIGURE 4: ORGANIZATION-WIDE CONTROL ALLOCATION

[40] When authorizing officials issue a *common control authorization* (see Appendix F), they are addressing the security and privacy risks to systems that can potentially inherit those controls. Authorizing officials that issue an *authorization to operate* or *authorization to use* also consider the security and privacy risks associated with the inheritance of the common controls identified by the organization for the system they are authorizing. Common control authorization addresses the risk in providing (i.e., provisioning) common controls to system owners. System authorization addresses the risk in receiving or using the inherited controls.

2.7 SECURITY AND PRIVACY POSTURE

The purpose of the RMF is to help ensure that, throughout the SDLC, information systems, organizations, and individuals are adequately protected, and that authorizing officials have the information needed to make credible, risk-based decisions regarding the operation or use of systems or the provision of common controls. A key aspect of risk-based decision making for authorizing officials is understanding the security and privacy posture of information systems and the common controls that are available for inheritance by those systems. The security and privacy posture represents the status of information systems and information resources (e.g., personnel, equipment, funds, and information technology) within an organization based on information assurance resources (e.g., people, hardware, software, policies, procedures) and the capabilities in place to manage the defense of the organization in its operation or use of systems; comply with applicable privacy requirements and manage privacy risks; and react as the situation changes.

The security and privacy posture of information systems and organizations is determined on an ongoing basis by assessing and continuously monitoring system-specific, hybrid, and common controls.[41] The control assessments and monitoring activities provide evidence that the controls selected by the organization are implemented correctly, operating as intended, and satisfying the security and privacy requirements in response to laws, executive orders, regulations, directives, policies, standards, or mission and business requirements. Authorizing officials use the security and privacy posture to determine if the risk to organizational operations and assets, individuals, other organizations, or the Nation are acceptable based on the organization's risk management strategy and organizational risk tolerance.[42]

2.8 SUPPLY CHAIN RISK MANAGEMENT

Organizations are becoming increasingly reliant on products, systems, and services provided by external providers to carry out missions and business functions. Organizations are responsible and accountable for the risk incurred when using such component products, systems, and services.[43] Relationships with external providers can be established in a variety of ways, for example, through joint ventures, business partnerships, various types of formal agreements (e.g., contracts, interagency agreements, lines of business arrangements, licensing agreements), or outsourcing arrangements.

The growing dependence on products, systems, and services from external providers, along with the nature of the relationships with those providers, present an increasing amount of risk to an organization. Some of these risks include the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the supply chain. Supply chain risks can be endemic or systemic within a system element or component, system, organization, sector, or nation. While the singular use of a component or service operated in a system may present an acceptable risk to an organization, its common use throughout a system, organization, sector or nation can raise the risk to an unacceptable level. These risks are associated with the global and distributed

[41] Monitoring of controls is part of an organization-wide risk management approach defined in [SP 800-39].

[42] See RMF *Prepare-Organization Level* step, Task P-2.

[43] [OMB A-130] defines supply chain risk and requires federal agencies to consider supply chain security issues for all resource planning and management activities throughout the SDLC so that risks are appropriately managed.

nature of product and service supply chains and an organization's decreased visibility into, and understanding of, how the technology that they acquire is developed, integrated, and deployed. This includes the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the acquired products, systems, and services.

To address supply chain risks, organizations develop an SCRM policy, which is an important vehicle for directing SCRM activities.[44] Guided and informed by applicable laws, executive orders, directives, policies, and regulations, the SCRM policy supports applicable organizational policies including, for example, acquisition and procurement, information security and privacy, quality, supply chain, and logistics. The policy addresses the goals and objectives established in the organization's strategic plan, specific missions and business functions, and the internal and external customer requirements. It also defines the integration points for SCRM with the risk management and the SDLC processes for the organization. The SCRM policy defines SCRM-related roles and responsibilities within the organization, any dependencies among those roles, and the interaction among the roles. SCRM roles specify the responsibilities for procurement, collecting supply chain threat intelligence, conducting risk assessments, identifying and implementing risk-based mitigations, and performing monitoring functions.

[FISMA14] and [OMB A-130] require external providers handling federal information or operating systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies. Security and privacy requirements for external providers including the controls for systems processing, storing, or transmitting federal information are expressed in contracts or other formal agreements. The RMF can be effectively used to manage supply chain security risk. The conceptual view of the system in Figure 3 can guide and inform security, privacy, and risk management activities for all elements of the supply chain. Every step in the RMF can be executed by nonfederal external providers except for the *Authorize* step—that is, the acceptance of risk is an inherent federal responsibility for which senior executives are held responsible and accountable. The authorization decision is directly linked to the management of risk related to the acquisition and use of component products, systems, and services from external providers.[45] [OMB A-130] also requires organizations to develop and implement SCRM plans.[46]

Managing supply chain risk is a complex, multifaceted undertaking requiring a coordinated effort across an organization—building trust relationships and communicating with both internal and external stakeholders. SCRM activities involve identifying and assessing applicable risks, determining appropriate mitigating actions, developing appropriate SCRM plans to document selected mitigating actions, and monitoring performance against SCRM plans. Because supply chains differ across and within organizations, SCRM plans are tailored to the individual program,

[44] [SP 800-161] provides guidance on SCRM practices. SCRM and security risk management share many common objectives with regard to protecting the confidentiality, integrity, and availability of information and information systems. However, there are also areas where SCRM diverges from traditional security risk management. SCRM policies are coordinated with information security policies at the organizational level to ensure that the policies are mutually supportive and reinforcing. The RMF tasks address those areas where SCRM and security risk management share common objectives.

[45] While *authorization* (i.e., the acceptance of risk) of federal information systems is an inherent federal responsibility, it is a foundational concept that can be used by senior executives in nonfederal organizations at all levels in the supply chain to manage security and privacy risk.

[46] [SP 800-161] provides guidance on SCRM plans.

organizational, and operational contexts. Tailored plans provide the basis for determining whether a system is “fit for purpose” and as such, the controls need to be tailored accordingly. Tailored SCRM plans help organizations to focus their resources on the most critical missions and business functions based on mission and business requirements and their risk environment.

The determination that the risk from acquiring products, systems, or services from external providers is acceptable depends on the level of assurance[47] that the organization can gain from the providers. The level of assurance is based on the degree of control the organization can exert on the external provider regarding the controls needed for the protection of the product, system, or service and the evidence brought forth by the provider as to the effectiveness of those controls.

The degree of control is established by the specific terms and conditions of the contract or service-level agreement. Some organizations have extensive control through contract vehicles or other agreements that specify the security and privacy requirements for the external provider. Other organizations, in contrast, have limited control because they are purchasing commodity services or commercial off-the-shelf products. The level of assurance can also be based on many other factors that convince the organization that the requisite controls have been implemented and that a credible determination of control effectiveness exists. For example, an authorized external cloud service provided to an organization through a well-established line-of-business relationship may provide a level of trust in the service that is within the risk tolerance of the organization. Ultimately, the responsibility for responding to risks from the use of component products, systems, and services from external providers remains with the organization and the authorizing official. Organizations require that an appropriate *chain of trust* be established with external providers when dealing with the many issues associated with system security or privacy risks.

SUPPLY CHAIN RISK MANAGEMENT PLANS

Organizations have flexibility on how the details of SCRM plans are documented. SCRM plan details for Levels 1 and 2 (organization and mission/business process levels), can be documented in the information security program plan for the organization or in separate organization-level and/or mission/business process-level SCRM plans. SCRM plan details for Level 3 (information system level) can be documented in the system security plan or in a separate system-level SCRM plan. A SCRM plan template is provided in [SP 800-161].

[47] The level of assurance provided by an external provider can vary, ranging from those who provide high assurance (e.g., business partners in a joint venture that share a common business model and goals) to those who provide less assurance and represent greater sources of risk (e.g., business partners in one endeavor who are also competitors in another market sector).

CHAPTER THREE

THE PROCESS

EXECUTING THE RISK MANAGEMENT FRAMEWORK TASKS

This chapter describes the steps and associated tasks that comprise the RMF and the selected individuals or groups (defined organizational roles) that carry out such tasks.[48] Many risk management roles defined in this publication have counterpart roles defined in the SDLC process. Organizations align their risk management roles with similar or complementary roles defined for the SDLC whenever possible, and consistent with missions and business functions. RMF tasks are executed concurrently with, or as part of, the SDLC processes in the organization. This helps to ensure that organizations are effectively integrating the process of managing information security, privacy, and supply chain risks with life cycle processes.

The process of implementing RMF tasks may vary from organization to organization. The tasks are applied at appropriate phases in the SDLC. While the tasks appear in sequential order, there can be many points in the risk management process that require divergence from the sequential order including the need for iterative cycles between initial task execution and revisiting tasks. For example, control assessment results can trigger a set of remediation actions by system owners and common control providers, which can in turn require the reassessment of selected controls. Monitoring controls can generate a cycle of tracking changes to the system and its environment of operation; assessing the information security and privacy impact; reassessing controls, taking remediation actions, and reporting the security and privacy posture of the system and the organization.

There may be other opportunities to diverge from the sequential nature of the tasks when it is more effective, efficient, or cost-effective to do so. For example, while the control assessment tasks are listed after the control implementation tasks, organizations may begin the assessment of controls as soon as they are implemented but prior to the complete implementation of all controls described in the security plans and privacy plans. This may result in some organizations assessing the physical and environmental protection controls within a facility prior to assessing the controls implemented in the hardware, firmware, or software components of the system (which may be implemented later). Regardless of the task ordering, the final action before a system is placed into operation is the explicit acceptance of risk by the authorizing official.

The RMF steps and associated tasks can be applied to new development systems and existing systems. For new and existing systems, organizations ensure that the designated tasks have been completed to prepare for the execution of the RMF. For existing systems, organizations confirm that the security categorization and (for information systems processing PII) a privacy risk assessment have been completed and are appropriate; and that the needed controls have been selected, tailored, and implemented.

[48] Appendix D describes the roles and responsibilities of key participants involved in organizational risk management and the execution of the RMF.

Applying the RMF steps and associated tasks to existing systems can serve as a gap analysis to determine if the organization's security and privacy risks have been effectively managed. Deficiencies in controls can be addressed in the RMF steps for implementation, assessment, authorization, and monitoring in the same manner as in new development systems. If no deficiencies are discovered during the gap analysis and there is a current authorization in effect, the organization can move directly to the continuous monitoring step in the RMF. If a current authorization is not in effect, the organization continues in the usual sequence with the assessment, authorization, and monitoring steps.

TIPS FOR STREAMLINING RMF IMPLEMENTATION

- Use the tasks and outputs of the Organization-Level and System-Level *Prepare* Step to promote a consistent starting point within organizations to execute the RMF.
- Maximize the use of *common controls* at the organization level to promote standardized, consistent, and cost-effective security and privacy capability inheritance.
- Maximize the use of *shared* or *cloud-based* systems, services, and applications to reduce the number of authorizations, enterprise-wide.
- Employ organization-wide *tailored* control baselines (including organization-wide control parameters) to increase the speed of security and privacy plan development and the consistency of security and privacy plan content.
- Employ organization-defined controls based on security and privacy requirements generated from a systems security engineering process;
- Maximize the use of *automated tools* to manage security categorization; control selection, assessment, and monitoring; and the authorization process.
- Decrease the level of effort and resource expenditures for *low-impact* systems if those systems cannot adversely affect higher-impact systems through system connections.
- Maximize the *reuse* of RMF artifacts (e.g., security and privacy assessment results) for standardized hardware/software deployments, including configuration settings.
- Reduce the *complexity* of the IT/OT infrastructure by eliminating unnecessary systems, system components, and services — employ *least functionality* principle.
- Make the transition to *ongoing authorization* a priority and use *continuous monitoring* approaches to reduce the cost and increase the efficiency of security and privacy programs.

1051

DEVELOPING WELL-DEFINED SECURITY AND PRIVACY REQUIREMENTS

The RMF is an SDLC-based process that can be effectively used to help ensure that security and privacy requirements are satisfied for information systems or organizations. Defining clear, consistent, and unambiguous security and privacy requirements is an important element in the successful execution of the RMF. The requirements are defined early in the SDLC in collaboration with the senior leaders and are integrated into the acquisition and procurement processes. For example, organizations can use the [SP 800-160-1] life cycle-based systems engineering process to define an initial set of security and privacy requirements, which in turn, can be used to select a set of controls* to satisfy the requirements. The requirements or the controls can be stated in the Request for Proposal or other contractual agreement when organizations acquire systems, system components, or services. Requirements can also be added throughout the life cycle, such as with the agile development methodology where new features are continuously deployed.

The NIST *Cybersecurity Framework* [NIST CSF] (i.e., Core, Profiles) can also be used to identify, align, and deconflict security requirements and to subsequently inform the selection of security controls for an organization. Cybersecurity Framework Profiles can provide a link between cybersecurity activities and organizational mission/business objectives, which supports risk-based decision-making throughout the RMF. While Profiles may be used as a starting point to inform control selection and tailoring activities, further evaluation is needed to ensure the appropriate controls are selected. Some organizations may choose to use the Cybersecurity Framework in concert with the NIST *Systems Security Engineering* publications—identifying, aligning, and deconflicting requirements across a sector, an industry, or an organization—and subsequently employing a systems engineering approach to further refine the requirements and obtain trustworthy secure solutions to help protect the organization's operations, assets, individuals.

* See Section 2.3 for specific guidance on privacy control selection and managing privacy risk.

ORGANIZATION AND SYSTEM PREPARATION

Preparation can achieve effective, efficient, and cost-effective execution of risk management processes. The primary objectives of the *Prepare* step include:

- Facilitate better communication between senior leaders and executives in the C-suite and system owners and operators—
  - aligning organizational priorities with resource allocation and prioritization at the system level; and
  - conveying acceptable limits regarding the selection and implementation of controls within the established organizational risk tolerance.
- Promote organization-wide identification of common controls and the development of organization-wide tailored control baselines, to reduce the workload on individual system owners and the cost of system development and protection.
- Reduce the complexity of the IT infrastructure by consolidating, standardizing, and optimizing systems, applications, and services through the application of enterprise architecture concepts and models.
- Identify, prioritize, and focus resources on high-value assets that require increased levels of protection.
- Facilitate system readiness for system-specific tasks.

These objectives, if achieved, significantly reduce the information technology footprint and the attack surface of organizations, promote IT modernization objectives, and prioritize security and privacy activities to focus protection strategies on the most critical assets and systems.

Finally, certain tasks in the *Prepare* step at the organization level are designated as *optional*. These tasks are included to provide organizations additional options to help make their RMF implementations more effective, efficient, and cost-effective.

3.1 PREPARE [49]

Purpose

The purpose of the ***Prepare*** step is to carry out essential activities at the organization, mission and business process, and information system levels of the enterprise to help prepare the organization to manage its security and privacy risks using the *Risk Management Framework*.

PREPARE TASKS—ORGANIZATION LEVEL [50]

Table 1 provides a summary of tasks and expected outcomes for the RMF *Prepare* step at the *organization* level. Applicable Cybersecurity Framework constructs are also provided.

TABLE 1: PREPARE TASKS AND OUTCOMES—ORGANIZATION LEVEL

Tasks	Outcomes
TASK P-1 RISK MANAGEMENT ROLES	- Individuals are identified and assigned key roles for executing the Risk Management Framework. [*Cybersecurity Framework*: **ID.AM-6**; **ID.GV-2**]
TASK P-2 RISK MANAGEMENT STRATEGY	- A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established. [*Cybersecurity Framework*: **ID.RM; ID.SC**]
TASK P-3 RISK ASSESSMENT—ORGANIZATION	- An organization-wide risk assessment is completed or an existing risk assessment is updated. [*Cybersecurity Framework*: **ID.RA; ID.SC-2**]
TASK P-4 ORGANIZATION-WIDE TAILORED CONTROL BASELINES AND PROFILES (OPTIONAL)	- Tailored control baselines for organization-wide use are established and made available. [*Cybersecurity Framework*: **Profile**]
TASK P-5 COMMON CONTROL IDENTIFICATION	- Common controls that are available for inheritance by organizational systems are identified, documented, and published.
TASK P-6 IMPACT-LEVEL PRIORITIZATION (OPTIONAL)	- A prioritization of organizational systems with the same impact level is conducted. [*Cybersecurity Framework*: **ID.AM-5**]
TASK P-7 CONTINUOUS MONITORING STRATEGY—ORGANIZATION	- An organization-wide strategy for monitoring control effectiveness is developed and implemented. [*Cybersecurity Framework*: **DE.CM; ID.SC-4**]

Quick link to summary table for RMF tasks, responsibilities, and supporting roles.

[49] The *Prepare* step is intended to leverage activities already being conducted within security, privacy, and supply chain programs to emphasize the importance of having enterprise-wide governance and the appropriate resources in place to enable the execution of cost-effective and consistent risk management processes across the organization.

[50] For ease of use, the preparatory activities are grouped into organization-level preparation and information system-level preparation.

RISK MANAGEMENT ROLES

TASK P-1 Identify and assign individuals to specific roles associated with security and privacy risk management.

Potential Inputs: Organizational security and privacy policies and procedures; organizational charts.

Potential Outputs: Documented Risk Management Framework role assignments.

Primary Responsibility: Head of Agency; Chief Information Officer; Senior Agency Official for Privacy.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Information Security Officer.

Discussion: The roles and responsibilities of key participants in risk management processes are described in Appendix D. The roles and responsibilities may include personnel that are internal or external to the organization, as appropriate. Since organizations have different missions, functions, and organizational structures, there may be differences in naming conventions for risk management roles and how specific responsibilities are allocated among organizational personnel including, for example, multiple individuals filling a single role or one individual filling multiple roles. In either situation, the basic risk management functions remain the same. Organizations ensure that there are no conflicts of interest when assigning the same individual to multiple risk management roles. For example, authorizing officials cannot occupy the role of system owner or common control provider for systems or common controls they are authorizing. In addition, combining multiple roles for security and privacy requires care because the two disciplines may require different expertise, and in some circumstances, the priorities may be competing. Some roles may be allocated to a group or an office rather than to an individual, for example, control assessor, risk executive (function), or system administrator.

References: [SP 800-160-1] (Human Resource Management Process); [SP 800-181]; [NIST CSF] (Core [Identify Function]).

RISK MANAGEMENT STRATEGY

TASK P-2 Establish a risk management strategy for the organization that includes a determination of risk tolerance.

Potential Inputs: Organizational mission statement; organizational policies; organizational risk assumptions, constraints, priorities and trade-offs.

Potential Outputs: Risk management strategy and statement of risk tolerance inclusive of information security and privacy risk.

Primary Responsibility: Head of Agency.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

Discussion: Risk tolerance is the degree of risk or uncertainty that is acceptable to an organization. Risk tolerance affects all components of the risk management process, having a direct impact on the risk management decisions made by senior leaders or executives throughout the organization and providing important constraints on those decisions. The risk management strategy guides and informs risk-based decisions including how security and privacy risk is framed, assessed, responded to, and monitored. The risk management strategy may be composed of a single document, or separate security and privacy risk management documents.[51] The risk management strategy makes explicit the threats, assumptions, constraints, priorities, trade-offs, and risk tolerance used for making investment and operational

[51] A separate supply chain risk management strategy document is called a *supply chain risk management plan*.

decisions. This strategy includes the strategic-level decisions and considerations for how senior leaders and executives are to manage security and privacy risks to organizational operations, organizational assets, individuals, other organizations, and the Nation. The risk management strategy includes an expression of organizational risk tolerance; acceptable risk assessment methodologies and risk response strategies; a process for consistently evaluating security and privacy risks across the organization; and approaches for monitoring risk over time. As organizations define and implement risk management strategies, policies, procedures, and processes, it is important that they include SCRM considerations. The risk management strategy for security and privacy connects security and privacy programs with the management control systems established in the organization's Enterprise Risk Management strategy.[52]

References: [SP 800-30]; [SP 800-39] (Organization Level); [SP 800-160-1] (Risk Management, Decision Management, Quality Assurance, Quality Management, Project Assessment and Control Processes); [SP 800-161]; [IR 8062]; [IR 8179] (Criticality Analysis Process B); [NIST CSF] (Core [Identify Function]).

RISK ASSESSMENT—ORGANIZATION

TASK P-3 Assess organization-wide security and privacy risk and update the results on an ongoing basis.

Potential Inputs: Risk management strategy; mission or business objectives; current threat information; system-level security and privacy risk assessment results; previous organization-level security and privacy risk assessment results; information sharing agreements or memoranda of understanding; security- and privacy-related information from continuous monitoring.

Potential Outputs: Organization-level risk assessment results.

Primary Responsibility: Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Information Security Officer; Senior Agency Official for Privacy.

Supporting Roles: Chief Information Officer; Mission or Business Owner; Authorizing Official or Authorizing Official Designated Representative.

Discussion: Risk assessment at the organizational level leverages aggregated information from system-level risk assessment results, continuous monitoring, and any strategic risk considerations relevant to the organization. The organization considers the totality of risk from the operation and use of its information systems, from information exchange and connections with other internally and externally owned systems, and from the use of external providers. For example, the organization may review the risk related to its enterprise architecture and information systems of varying impact levels residing on the same network and whether higher impact systems are segregated from lower impact systems or systems operated and maintained by external providers. Risk assessments of the organization's supply chain may be conducted as well. Risk assessment results may be used to help organizations establish a Cybersecurity Framework target profile.

References: [SP 800-30]; [SP 800-39] (Organization Level, Mission/Business Process Level); [SP 800-161]; [IR 8062].

TAILORED CONTROL BASELINES AND PROFILES[53]

TASK P-4 Establish, document, and publish organization-wide tailored control baselines and/or profiles.

[52] See [OMB A-123].

[53] Optional task.

Potential Inputs: Documented security and privacy requirements; requiring the use of specific tailored control baselines; mission or business objectives; organization- and system-level risk assessment results; NIST Special Publication 800-53B control baselines.[54]

Potential Outputs: List of organization-approved or mandated tailored baselines; [NIST CSF] profiles.

Primary Responsibility: Mission or Business Owner; Senior Accountable Official for Risk Management or Risk Executive (Function).

Supporting Roles: Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

Discussion: To address the organizational need for specialized sets of controls, tailored control baselines may be developed for organization-wide use.[55] An organization-wide tailored baseline provides a fully specified set of controls, control enhancements, and supplemental guidance derived from established control baselines described in [SP 800-53B]. The tailoring process can also be guided and informed by the requirements engineering process described in [SP 800-160-1]. Organizations can use the tailored control baseline concept when there is divergence from the specific assumptions used to create the initial control baselines in [SP 800-53B]. This would include, for example, situations when the organization has specific security or privacy risks, has specific mission or business needs, or plans to operate in environments that are not addressed in the initial baselines.

Tailored baselines and overlays complement the initial NIST control baselines by providing an opportunity to add or eliminate controls to accommodate organizational requirements while continuing to protect information commensurate with risk. Organizations can use tailored baselines to customize control baselines by describing control applicability and by providing interpretations for specific technologies; types of missions or business functions, operations, systems, operating modes, or environments of operation; and statutory or regulatory requirements. Multiple customized baselines may be useful for organizations with heterogeneous systems (e.g., organizations that maintain systems with different operating or processing characteristics, or mission or business characteristics).

Organization-wide tailored baselines can establish organization-defined control parameter values for assignment or selection statements in controls and control enhancements that are agreeable to specific communities of interest and can also extend the supplemental guidance where necessary. Organization-wide tailored baselines may be more stringent or less stringent than the baselines identified in [SP 800-53B] and are applied to multiple systems. Tailored baselines may also be mandated for use by certain laws, executive orders, directives, regulations, policies, or standards. In some situations, tailoring actions may be restricted or limited by the developer of the tailored baseline or by the issuing authority for the tailored baseline. Tailored baselines (or overlays) have been developed by communities of interest for cloud and shared systems, services, and applications; industrial control systems; national security systems; weapons and space-based systems; high-value assets; mobile device management; federal public key infrastructure; and privacy risks.

Organizations may also benefit from the creation of one or more Cybersecurity Framework *profiles*. A profile is a prioritization of the Framework Core Categories or Subcategory outcomes based on mission or business functions, security requirements, and risk determinations. The prioritized list of cybersecurity outcomes developed at the organization and mission/business process levels can be helpful in facilitating consistent, risk-based decisions at the system level. Profiles, the precursor to subcategory selection in the

[54] NIST Special Publication 800-53 (Revision 5), separates the control catalog from the control baselines that have been included historically in that publication. A new companion publication, NIST Special Publication 800-53B, *Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations* is forthcoming. This publication is referenced throughout the RMF in the relevant tasks.

[55] Tailored control baselines may also be referred to as *overlays*. An organization-wide tailored control baseline is analogous to an organization-wide overlay since an overlay is a tailored baseline that services a community of interest, in this case, the organization.

Cybersecurity Framework, can also be used to guide and inform the development of the tailored control baselines described above.

References: [SP 800-53]; [SP 800-53B]; [SP 800-160-1] (Business or Mission Analysis and Stakeholder Needs and Requirements Definition Processes); [NIST CSF] (Core, Profiles).

COMMON CONTROL IDENTIFICATION

TASK P-5 Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems.

Potential Inputs: Documented security and privacy requirements; existing common control providers and associated security and privacy plans; information security and privacy program plans; organization- and system-level security and privacy risk assessment results.

Potential Outputs: List of common control providers and common controls available for inheritance; security and privacy plans (or equivalent documents) providing a description of the common control implementation (including inputs, expected behavior, and expected outputs).

Primary Responsibility: Senior Agency Information Security Officer; Senior Agency Official for Privacy.

Supporting Roles: Mission or Business Owner; Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative; Common Control Provider; System Owner.

Discussion: Common controls are controls that can be inherited by one or more information systems. Common controls can include controls from any [SP 800-53] control family, for example, physical and environmental protection controls, system boundary and monitoring controls, personnel security controls, policies and procedures, acquisition controls, account and identity management controls, audit log and accountability controls, or complaint management controls for receiving privacy-related inquiries from the public. Organizations identify and select the set of common controls and allocate those controls to the organizational entities designated as common control providers. Common controls may differ based upon a variety of factors, such as hosting location, system architecture, and the structure of the organization. The organization-wide list of common controls takes these factors into account. Common controls can also be identified at different levels of the organization, including, for example, corporate, department, or agency level; bureau or subcomponent level; or individual program level. Organizations may establish one or more lists of common controls that can be inherited by information systems. A particular requirement may not be fully met by a common control. In such cases, the control is considered a hybrid control and is noted as such by the organization, including specifying which parts of the control requirement are provided for inheritance by the common control and which parts are to be provided at the system level.

When there are multiple sources of common controls, organizations specify the common control provider (i.e., who is providing the controls and through what venue, for example, shared services, specific systems, or within a specific type of architecture) and which systems or types of systems can inherit the controls. Common control listings are communicated to system owners so they are aware of the security and privacy capabilities that are available from the organization through inheritance. System owners are not required to assess common controls that are inherited by their systems or document common control implementation details; that is the responsibility of the common control providers. Likewise, common control providers are not required to have visibility into the system-level details of those systems that are inheriting the common controls they are providing.

Risk assessment results can be used when identifying common controls to determine if the controls available for inheritance satisfy the security and privacy requirements for organizational systems and the environments in which those systems operate (including the identification of potential single points of failure). When the common controls provided by the organization are determined to be insufficient for the information systems inheriting those controls, system owners can supplement the common controls with system-specific or hybrid controls to achieve the required protection for their systems or accept greater risk with the acknowledgement and approval of the organization.

Common control providers execute the RMF steps to implement, assess, and monitor the controls designated as common controls. Common control providers may also be system owners when the common controls are resident within an information system. Organizations select senior officials or executives to serve as authorizing officials for common controls. The senior agency official for privacy is responsible for designating common privacy controls and for documenting them in the organization's privacy program plan. Authorizing officials are responsible for accepting security and privacy risk resulting from the use of common controls inherited by organizational systems.

Common control providers are responsible for documenting common controls in security and privacy plans (or equivalent documents prescribed by the organization); ensuring that the common controls are implemented and assessed for effectiveness by qualified assessors and that assessment findings are documented in assessment reports; producing a plan of action and milestones for common controls determined to have unacceptable deficiencies and targeted for remediation; receiving authorization for the common controls from the designated authorizing official; and monitoring control effectiveness on an ongoing basis. Plans, assessment reports, and plans of action and milestones for common controls (or a summary of such information) are made available to system owners and can be used by authorizing officials to guide and inform authorization decisions for systems inheriting common controls. For information about the authorization of common controls, see Task R4 and Appendix F.

References: [SP 800-53].

IMPACT-LEVEL PRIORITIZATION [56]

TASK P-6 Prioritize organizational systems with the same impact level.

Potential Inputs: System categorization information for organizational systems; system descriptions; organization- and system-level risk assessment results; mission or business objectives; Cybersecurity Framework profiles.

Potential Outputs: Organizational systems prioritized into low-, moderate-, and high-impact sub-categories.

Primary Responsibility: Senior Accountable Official for Risk Management or Risk Executive (Function).

Supporting Roles: Senior Agency Information Security Officer; Senior Agency Official for Privacy; Mission or Business Owner; System Owner; Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative.

Discussion: This task is carried out *only* after organizational systems have been categorized (see Task C1). This task requires organizations to first apply the "high water mark" concept to each of their information systems categorized in accordance with [FIPS 199]. The application of the high-water mark concept results in systems designated as low impact, moderate impact, or high impact. Organizations desiring additional granularity in their impact designations for risk-based decision making can use this task to prioritize their systems within each impact level. For example, an organization may decide to prioritize its moderate-impact systems by assigning each moderate system to one of three new subcategories: *low-moderate* systems, *moderate-moderate* systems, and *high-moderate* systems. The prioritization of its moderate systems gives organizations an opportunity to make more informed decisions regarding control selection and the tailoring of control baselines when responding to identified risks.[57] Impact-level prioritization can

[56] Optional task.

[57] Organizations can use this task in conjunction with the optional RMF *Prepare*-Organization Level step, Task P4, to develop organization-wide tailored baselines for the more granular impact designations, for example, organization-wide tailored baselines for low-moderate systems and high-moderate systems.

also be used to determine those systems that are critical or essential to organizational missions and business operations and therefore, organizations can focus on the factors of complexity, aggregation, and system interconnections. Such systems can be identified, for example, by prioritizing high-impact systems into *low-high* systems, *moderate-high* systems, and *high-high* systems. Impact-level prioritizations can be conducted at any level of the organization and are based on system categorization data reported by individual system owners. Impact-level prioritization may necessitate the development of organization-wide tailored baselines to designate the appropriate set of controls for the additional, more granular impact levels.

References: [FIPS 199]; [SP 800-30]; [SP 800-39] (Organization and System Levels); [SP 800-59]; [SP 800-60-1]; [SP 800-60-2]; [SP 800-160-1] (System Requirements Definition Process); [IR 8179] (Criticality Analysis Process B); [CNSSI 1253]; [NIST CSF] (Core [Identify Function]).

CONTINUOUS MONITORING STRATEGY—ORGANIZATION

TASK P-7 Develop and implement an organization-wide strategy for continuously monitoring control effectiveness.

Potential Inputs: Risk management strategy; organization- and system-level risk assessment results; organizational security and privacy policies.

Potential Outputs: An implemented organizational continuous monitoring strategy.

Primary Responsibility: Senior Accountable Official for Risk Management or Risk Executive (Function).

Supporting Roles: Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Mission or Business Owner; System Owner; Authorizing Official or Authorizing Official Designated Representative.

Discussion: An important aspect of risk management is the ability to monitor the security and privacy posture across the organization and the effectiveness of controls implemented within or inherited by organizational systems on an ongoing basis.[58] An effective organization-wide continuous monitoring strategy is essential to efficiently and cost-effectively carry out such monitoring. Continuous monitoring strategies can also include supply chain risk considerations, for example, regularly reviewing supplier foreign ownership, control, or influence (FOCI), monitoring inventory forecasts, or requiring on-going audits of suppliers. The implementation of a robust and comprehensive continuous monitoring program helps an organization understand the security and privacy posture of its information systems. It also facilitates ongoing authorization after the initial system or common control authorizations. This includes the potential for changing missions or business functions, stakeholders, technologies, vulnerabilities, threats, risks, and suppliers of systems, components, or services.

The organizational continuous monitoring strategy addresses monitoring requirements at the organization, mission/business process, and information system levels. The continuous monitoring strategy identifies the minimum monitoring frequency for implemented controls across the organization; defines the ongoing control assessment approach; and describes how ongoing assessments are to be conducted (e.g., addressing the use and management of automated tools, and instructions for ongoing assessment of controls for which monitoring cannot be automated). The continuous monitoring strategy may also define security and privacy reporting requirements including recipients of the reports.

The criteria for determining the minimum frequency for control monitoring post implementation, is established in collaboration with selected organizational officials including, for example, the senior accountable official for risk management or risk executive (function); senior agency information security

[58] Monitoring for control effectiveness is a form of control assessment. [SP 800-53A], [SP 800-137], and [IR 8011-1] provide additional information on monitoring, conducting control effectiveness assessments, and automating control effectiveness assessments respectively.

officer; senior agency official for privacy; chief information officer; system owners; common control providers; and authorizing officials or their designated representatives. An organizational risk assessment can be used to guide and inform the frequency of monitoring.

The use of automation facilitates a greater frequency and volume of control assessments as part of the monitoring process. The ongoing monitoring of controls using automated tools and supporting databases facilitates near real-time risk management for information systems and supports ongoing authorization and efficient use of resources. The senior accountable official for risk management or the risk executive (function) approves the continuous monitoring strategy including the minimum frequency with which controls are to be monitored.

References: [SP 800-30]; [SP 800-39] (Organization, Mission or Business Process, System Levels); [SP 800-53]; [SP 800-53A]; [SP 800-137]; [SP 800-161]; [IR 8062]; [NIST CSF] (Core [Detect Function]); [CNSSI 1253].

MISSION/BUSINESS PROCESS (LEVEL 2) CONSIDERATIONS

Mission/business process considerations are addressed in the RMF *Prepare-Organization Level* step and the RMF *Prepare-System Level* step by specifying mission/business process concerns; by identifying the mission or business owners in primary or supporting roles; and by identifying the mission or business objectives. Task P-8 and Task P-9 from the RMF *Prepare-System Level* step are mission/business process level tasks conducted with a system-level specific focus.

PREPARE TASKS—SYSTEM LEVEL

Table 2 provides a summary of tasks and expected outcomes for the RMF *Prepare* step at the *system* level. Applicable Cybersecurity Framework constructs are also provided.

TABLE 2: PREPARE TASKS AND OUTCOMES—SYSTEM LEVEL

Tasks	Outcomes
TASK P-8 MISSION OR BUSINESS FOCUS	• Missions, business functions, and mission/business processes that the system is intended to support are identified. [*Cybersecurity Framework*: **Profile**; **Implementation Tiers**; **ID.BE**]
TASK P-9 SYSTEM STAKEHOLDERS	• The stakeholders having an interest in the system are identified. [*Cybersecurity Framework*: **ID.AM**; **ID.BE**]
TASK P-10 ASSET IDENTIFICATION	• Stakeholder assets are identified and prioritized. [*Cybersecurity Framework*: **ID.AM**]
TASK P-11 AUTHORIZATION BOUNDARY	• The authorization boundary (i.e., system) is determined.
TASK P-12 INFORMATION TYPES	• The types of information processed, stored, and transmitted by the system are identified. [*Cybersecurity Framework*: **ID.AM-5**]
TASK P-13 INFORMATION LIFE CYCLE	• Identify and understand all stages of the information life cycle.
TASK P-14 RISK ASSESSMENT—SYSTEM	• A system-level risk assessment is completed or an existing risk assessment is updated. [*Cybersecurity Framework*: **ID.RA; ID.SC-2**]
TASK P-15 SECURITY AND PRIVACY REQUIREMENTS	• Security and privacy requirements are defined and prioritized. [*Cybersecurity Framework*: **ID.GV; PR.IP**]

Tasks	Outcomes
TASK P-16 ENTERPRISE ARCHITECTURE	- The placement of the system within the enterprise architecture is determined.
TASK P-17 SYSTEM REGISTRATION	- The system is registered for purposes of management, accountability, coordination, and oversight. [*Cybersecurity Framework*: **ID.GV**]

Quick link to summary table for RMF tasks, responsibilities, and supporting roles.

MISSION OR BUSINESS FOCUS

TASK P-8 Identify the missions, business functions, and mission/business processes that the system is intended to support.

Potential Inputs: Organizational mission statement; organizational policies; mission/business process information; system stakeholder information; Cybersecurity Framework profiles.

Potential Outputs: Missions, business functions, and mission/business processes that the system will support.

Primary Responsibility: Mission or Business Owner.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; System Owner; Information Owner or Steward; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

System Life Development Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Organizational missions and business functions influence the design and development of the mission or business processes that are created to carry out those missions and business functions. The prioritization of missions and business functions drives investment strategies and funding decisions, and therefore, affects the development of the enterprise architecture and the associated security and privacy architectures. Information is elicited from stakeholders to acquire a more thorough understanding of the missions, business functions, and mission/business processes of the organization from a system security and privacy perspective.

References: [SP 800-39] (Organization and Mission/Business Process Levels); [SP 800-64]; [SP 800-160-1] (Business or Mission Analysis, Portfolio Management, and Project Planning Processes); [NIST CSF] (Core [Identify Function]); [IR 8179] (Criticality Analysis Process B).

SYSTEM STAKEHOLDERS

TASK P-9 Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.

Potential Inputs: Organizational mission statement; mission or business objectives; missions, business functions, and mission/business processes that the system will support; other mission/business process information; organizational security and privacy policies and procedures; organizational charts; information about individuals or groups (internal and external) that have an interest in and decision-making responsibility for the system.

Potential Outputs: List of system stakeholders.

Primary Responsibility: Mission or Business Owner; System Owner.

Supporting Roles: Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative; Information Owner or Steward; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Chief Acquisition Officer.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Stakeholders include individuals, organizations, or representatives that have an interest in the system throughout the system life cycle—for design, development, implementation, delivery, operation, and sustainment of the system. It also includes all aspects of the supply chain. Stakeholders may reside in the same organization or they may reside in different organizations in situations when there is a common interest by those organizations in the information system. For example, this may occur during the development, operation, and maintenance of cloud-based systems, shared service systems, or any system where organizations may be adversely impacted by a breach or a compromise to the system or for a variety of considerations related to the supply chain. Communication among stakeholders is important during every step in the RMF and throughout the SDLC to ensure that security and privacy requirements are satisfied, concerns and issues are addressed expeditiously, and risk management processes are carried out effectively.

References: [SP 800-39] (Organization Level); [SP 800-64]; [SP 800-160-1] (Stakeholder Needs and Requirements Definition and Portfolio Management Processes); [SP 800-161]; [NIST CSF] (Core [Identify Function]).

ASSET IDENTIFICATION

TASK P-10 Identify assets that require protection.

Potential Inputs: Missions, business functions, and mission/business processes the information system will support; business impact analyses; internal stakeholders; system stakeholder information; system information; information about other systems that interact with the system.

Potential Outputs: Set of assets to be protected.

Primary Responsibility: System Owner.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Mission or Business Owner; Information Owner or Steward; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Assets are tangible and intangible items that are of value to achievement of mission or business objectives. Tangible assets are physical in nature and include physical/environmental elements (e.g., non-digital information, structures, facilities), human elements, and technology/machine elements (e.g., hardware elements of components, mechanisms, and networks). In contrast, intangible assets are not physical in nature and include mission and business processes, functions, digital information and data, firmware, software, and services. Information assets include the information needed to carry out missions or business functions, to deliver services, and for system management/operation; controlled unclassified information and classified information; and all forms of documentation associated with the information system. Intangible assets can also include the image or reputation of an organization, and the privacy interests of the individuals whose information will be processed by the system. The organization defines the scope of stakeholder assets to be considered for protection. The assets that require protection are identified based on stakeholder concerns and the contexts in which the assets are used. This includes the missions or business functions of the organization; the other systems that interact with the system; and stakeholders whose assets are utilized by the mission or business functions or by the system.

References: [SP 800-39] (Organization Level); [SP 800-64]; [SP 800-160-1] (Stakeholder Needs and Requirements Definition Process); [IR 8179] (Criticality Analysis Process C); [NIST CSF] (Core [Identify Function]); [NARA CUI].

AUTHORIZATION BOUNDARY

TASK P-11 Determine the authorization boundary of the system.

Potential Inputs: System design documentation; system stakeholder information; asset information; organizational structure information/charts.

Potential Outputs: Documented authorization boundary.

Primary Responsibility: Authorizing Official.

Supporting Roles: Chief Information Officer; System Owner; Mission or Business Owner; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Enterprise Architect.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Authorization boundaries establish the scope of protection for information systems (i.e., what the organization agrees to protect under its management control or within the scope of its responsibilities). Authorization boundaries are determined by authorizing officials with input from the system owner based on mission, management, or budgetary responsibility. A clear delineation of authorization boundaries is important for accountability and for security categorization, especially in situations where lower-impact systems are connected to higher-impact systems, or when external providers are responsible for the operation or maintenance of a system. Each system includes a set of elements (i.e., information resources)[59] organized to achieve one or more purposes and to support the organization's missions and business processes. Each system element is implemented in a way that allows the organization to satisfy specified security and privacy requirements. System elements include human elements, technology/machine elements, and physical/environmental elements.

The term system is used to define the set of system elements, system element interconnections, and the environment that is the focus of the RMF implementation (see FIGURE 3). The system is included in a single authorization boundary to ensure accountability. For systems processing PII, the privacy and security programs collaborate to develop a common understanding of authorization boundaries. To conduct effective risk assessments and select appropriate controls, privacy and security programs provide a clear and consistent understanding of what constitutes the authorization boundary. Understanding the authorization boundary and what will occur beyond it may influence controls selected and how they are implemented. For example, if a function of the system includes sharing PII externally, robust encryption controls may be selected for PII transmitted from the system.

Similarly, for systems either partially or wholly managed, maintained, or operated by external providers, an agreement clearly describing authorization boundaries ensures accountability. Privacy and security programs collaborate with providers to develop a common understanding of authorization boundaries. Formal agreements with external providers (e.g. contracts) may be used to delineate what constitutes authorization boundaries. Understanding such boundaries facilitates the selection of appropriate controls to manage supply chain risk.

References: [SP 800-18]; [SP 800-39] (System Level); [SP 800-47]; [SP 800-64]; [SP 800-160-1] (System Requirements Definition Process); [NIST CSF] (Core [Identify Function]).

[59] *System elements* are implemented via hardware, software, or firmware; physical structures or devices; or people, processes, and procedures. The term *system component* is used to indicate system elements that are implemented specifically via hardware, software, and firmware.

INFORMATION TYPES

TASK P-12 Identify the types of information to be processed, stored, and transmitted by the system.

Potential Inputs: Assets to be protected; mission/business process information.

Potential Outputs: A list of information types for the system.

Primary Responsibility: System Owner; Information Owner or Steward.

Supporting Role: Mission or Business Owner; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Identifying the types of information needed to support organizational missions, business functions, and mission/business processes is an important step in developing security and privacy plans for the system and a precondition for determining the security categorization. [NARA CUI] defines the information types that require protection as part of its Controlled Unclassified Information (CUI) program, in accordance with laws, regulations, or governmentwide policies. Organizations may define additional information types needed to support organizational missions, business functions, and mission/business processes that are not defined in the CUI Registry or in [SP 800-60-2].

References: [SP 800-39] (System Level); [SP 800-60-1]; [SP 800-60-2]; [NIST CSF] (Core [Identify Function]); [NARA CUI].

INFORMATION LIFE CYCLE

TASK P-13 Identify and understand all stages of the information life cycle.

Potential Inputs: Missions, business functions, and mission/business processes the system will support; system stakeholder information; information about other systems that interact with the system; system design documentation; list of information types.

Potential Outputs: Documentation of the stages though which information passes in the system, such as a data map or model illustrating how information is structured or is processed by the system throughout its life cycle. Such documentation includes, for example, data flow diagrams, entity relationship diagrams, database schemas, and data dictionaries.

Primary Responsibility: Senior Agency Official for Privacy; System Owner; Information Owner or Steward.

Supporting Roles: Chief Information Officer; Mission or Business Owner.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: The information life cycle describes the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion [OMB A-130]. Identifying and understanding all stages of the life cycle helps inform the organization's security and privacy risk assessments and the selection and implementation of controls.

Identifying the life cycle of information by using tools such as a data map enables organizations to understand how the information is being processed so that organizations can better assess where security and privacy risks could arise and where controls could be applied most effectively. It is important for organizations to consider the appropriate delineation of the authorization boundary and the information system's interaction with other systems because the way information enters and leaves the system can significantly affect the security and privacy risk assessments. The components of the system are identified with sufficient granularity to support such risk assessments.

Identifying and understanding the information life cycle is particularly relevant for the assessment of security and privacy risks since information may be processed by a system in any of the SDLC phases. For example, in the testing and integration phase of the SDLC, processing actual (i.e., live) data would likely raise security and privacy risks, but using substitute (i.e., synthetic) data may allow an equivalent benefit in terms of system testing while reducing risk.

References: [OMB A-130]; [OMB M-13-13]; [IR 8062].

RISK ASSESSMENT—SYSTEM

TASK P-14 Conduct a system-level risk assessment and update the risk assessment on an ongoing basis.

Potential Inputs: Assets to be protected; missions, business functions, and mission/business processes the system will support; business impact analyses or criticality analyses; system stakeholder information; information about other systems that interact with the system; provider information; threat information; data map; system design documentation; Cybersecurity Framework profiles; risk management strategy; organization-level risk assessment results.

Potential Outputs: Security and privacy risk assessment reports.

Primary Responsibility: System Owner; System Privacy Officer.[60]

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Authorizing Official or Authorizing Official Designated Representative; Mission or Business Owner; Information Owner or Steward; System Security Officer; Control Assessor.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: This task may require that organizations conduct security and privacy risk assessments to ensure that each type of risk is fully assessed. Assessment of security risk includes identification of threat sources[61] and threat events affecting assets, whether and how the assets are vulnerable to the threats, the likelihood that an asset vulnerability will be exploited by a threat, and the impact (or consequence) of loss of the assets. As a key part of the risk assessment, assets are prioritized based on the adverse impact or consequence of asset loss. The meaning of loss is defined for each asset type to enable a determination of the loss consequence (i.e., the adverse impact of the loss). Loss consequences may be tangible (e.g., monetary) or intangible (e.g., reputation) and constitute a continuum that spans from partial loss to total loss relative to the asset. Interpretations of information loss may include loss of possession, destruction, or loss of precision or accuracy. The loss of a function or service may be interpreted as a loss of control, loss of accessibility, loss of the ability to deliver normal function, performance, or behavior, or a limited loss of capability resulting in a level of degradation of function, performance, or behavior. Prioritization of assets is based on asset value, criticality, cost of replacement, impact on image or reputation, or trust by users, by mission or business partners, or by collaborating organizations. The asset priority translates to precedence in allocating resources, determining strength of mechanisms, and defining levels of assurance. Asset valuation is a precondition for defining security requirements.

Privacy risk assessments are conducted to determine the likelihood that a given operation the system is taking when processing PII could create an adverse effect on individuals—and the potential impact on individuals.[62] These adverse effects can arise from unauthorized activities that lead to the loss of confidentiality, integrity, or availability in information systems processing PII, or may arise as a byproduct

[60] System Privacy Officer is only a primary role when the information system processes PII.

[61] In addition, the use of threat intelligence, threat analysis, and threat modelling can help agencies develop the security capabilities necessary to reduce agency susceptibility to a variety of threats including hostile cyber-attacks, equipment failures, natural disasters, and errors of omission and commission.

[62] [IR 8062] introduces privacy risk management and a privacy risk model for conducting privacy risk assessments.

of authorized activities. Privacy risk assessments are influenced by contextual factors. Contextual factors can include, but are not limited to, the sensitivity level of the PII, including specific elements or in aggregate; the types of organizations using or interacting with the system and individuals' perceptions about the organizations with respect to privacy; individuals' understanding about the nature and purpose of the processing; and the privacy interests of individuals, technological expertise or demographic characteristics that influence their understanding or behavior. The privacy risks to individuals may affect individuals' decisions to engage with the system thereby impacting mission or business objectives, or create legal liability, reputational risks, or other types of risks for the organization. Impacts to the organization are not privacy risks. However, these impacts can guide and inform organizational decision-making and influence prioritization and resource allocation for risk response.

Risk assessments are also conducted to determine the potential that the use of an external provider for the development, implementation, maintenance, management, operation, or disposition of a system, system component, or service could create a loss, and the potential impact of that loss. The impact may be immediate (e.g., physical theft) or on-going (e.g., the ability of adversaries to replicate sensitive equipment because of theft). The impact may be endemic (e.g., limited to a single system) or systemic (e.g., including any system that uses a specific type of system component). Supply chain risk assessments consider vulnerabilities which may arise related to the disposition of a system or system element and from the use of external providers. Vulnerabilities in the supply chain may include a lack of traceability or accountability leading to the potential use of counterfeits, insertion of malware, or poor-quality systems. The use of external providers may result in a loss of visibility and control over how systems, system components, and services are developed, deployed, and maintained. A clear understanding of the threats, vulnerabilities, and potential impacts of an adverse supply chain-related event can help organizations appropriately balance supply chain risk with risk tolerance. Supply chain risk assessments can include information from supplier audits, reviews, and supply chain intelligence. Organizations develop a strategy for collecting information, including a strategy for collaborating with providers on supply chain risk assessments. Such collaboration helps organizations leverage information from providers, reduce redundancy, identify potential courses of action for risk responses, and reduce the burden on providers.

Risk assessments are conducted throughout the SDLC and support various RMF steps and tasks. Risk assessment results are used to inform potential courses of action for risk responses. Organizations determine the form of risk assessment conducted (including the scope, rigor, and formality of such assessments) and method of reporting results.

References: [FIPS 199]; [FIPS 200]; [SP 800-30]; [SP 800-39] (Organization Level); [SP 800-59]; [SP 800-60-1]; [SP 800-60-2]; [SP 800-64]; [SP 800-160-1] (Stakeholder Needs and Requirements Definition and Risk Management Processes); [SP 800-161] (Assess); [IR 8062]; [IR 8179]; [NIST CSF] (Core [Identify Function]); [CNSSI 1253].

REQUIREMENTS

TASK P-15 Define the security and privacy requirements for the system and the environment of operation.

Potential Inputs: System design documentation; organization- and system-level risk assessment results; known set of stakeholder assets to be protected; missions, business functions, and mission/business processes the system will support; business impact analyses or criticality analyses; system stakeholder information; data map of the information life cycle for PII; Cybersecurity Framework profiles; information about other systems that interact with the system; supply chain information; threat information; laws, executive orders, directives, regulations, or policies that apply to the system; risk management strategy.

Potential Outputs: Documented stakeholder protection needs; security and privacy requirements.

Primary Responsibility: Mission or Business Owner; System Owner; Information Owner or Steward; System Privacy Officer.[63]

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; System Security Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Chief Acquisition Officer.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Prior to defining security and privacy requirements, stakeholder protection needs are established. The protection needs are an expression of the protection capability required for the system. Protection needs include the security characteristics[64] of the system and the security behavior of the system in its intended operational environment and across all system life cycle phases. The protection needs reflect the relative priorities of stakeholders, results of negotiations among stakeholders in response to conflicts, opposing priorities, contradictions, and stated objectives, and thus, are inherently subjective. The protection needs are documented to help ensure that the reasoning, assumptions, and constraints associated with those needs are available for future reference and to provide traceability to the security and privacy requirements. Security and privacy requirements[65] constitute a formal, more granular expression of protection needs across all SDLC phases, the associated life cycle processes, and protections for the assets associated with the system. Security and privacy requirements are obtained from many sources including, for example, laws, executive orders, directives, regulations, policies, standards, mission and business needs, or risk assessments. These requirements are an important part of the formal expression of the required characteristics of the system, encompassing security and privacy.[66] The security and privacy requirements guide and inform the selection of controls for a system and the tailoring activities associated with those controls.

Organizations can use the Cybersecurity Framework to manage security and privacy requirements and express those requirements in Framework Profiles defined for the organization. For instance, multiple requirements can be aligned and even deconflicted using the *Function-Category-Subcategory* structure of the Framework Core. The Framework *profiles* can then be used to inform the development of tailored control baselines described in the RMF *Prepare-Organization Level* step, Task P-4.

References: [SP 800-39] (Organization Level); [SP 800-64]; [SP 800-160-1](Stakeholder Needs and Requirements Definition Process); [SP 800-161] (Multi-Tiered Risk Management); [IR 8179]; [NIST CSF] (Core [Protect, Detect, Respond, Recover Functions]; Profiles).

ENTERPRISE ARCHITECTURE

TASK P-16 Determine the placement of the system within the enterprise architecture.

Potential Inputs: Security and privacy requirements; organization- and system-level risk assessment results; enterprise architecture information; security architecture information; privacy architecture information; asset information.

[63] The system privacy officer is only a primary role when the information system processes PII.

[64] For example, a fundamental security characteristic is that the system exhibits only specified behaviors, interactions, and outcomes.

[65] The term *requirements* can have discrete meanings. For example, legal and policy requirements impose obligations to which organizations must adhere. Security and privacy requirements, however, are derived from the protection needs for the system and those protection needs can derive from legal or policy requirements, mission or business needs, risk assessments, or other sources.

[66] Security and privacy requirements can also include *assurance* requirements. Assurance is having confidence about the ability of the system to remain trustworthy with respect to security and privacy across all forms of adversity resulting from malicious or non-malicious intent.

Potential Outputs: Updated enterprise architecture; updated security architecture; updated privacy architecture; plans to use cloud-based systems and shared systems, services, or applications.

Primary Responsibility: Mission or Business Owner; Enterprise Architect; Security Architect; Privacy Architect.

Supporting Roles: Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative; Senior Agency Information Security Officer; Senior Agency Official for Privacy; System Owner; Information Owner or Steward.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: System complexity can impact risk and the ability of organizations to successfully carry out their missions and business functions. An enterprise architecture can help provide greater understanding of information and operational technologies included in the initial design and development of information systems and is a prerequisite for achieving resilience and survivability of those systems in an environment of increasingly sophisticated threats. Enterprise architecture is a management practice used to maximize the effectiveness of mission/business processes and information resources and to achieve mission and business success. Enterprise architecture provides a singular opportunity for organizations to consolidate, standardize, and optimize information and technology assets. An effectively implemented architecture produces systems that are more transparent and therefore, easier to understand and protect. Enterprise architecture also establishes an unambiguous connection from investments to measurable performance improvements. The placement of a system within the enterprise architecture is important as it provides greater visibility and understanding about the other systems (internal and external) that are connected to the system and can also be used to establish security domains for increased levels of protection for the system.

The security architecture and the privacy architecture are integral parts of the enterprise architecture. These architectures represent the parts of the enterprise architecture related to the implementation of security and privacy requirements. The primary purpose of the security and privacy architectures is to ensure that security and privacy requirements are consistently and cost-effectively met in organizational systems and are aligned with the risk management strategy. The security and privacy architectures provide a roadmap that facilitates traceability from the strategic goals and objectives of organizations, through protection needs and security and privacy requirements, to specific security and privacy solutions provided by people, processes, and technologies.

References: [SP 800-39] (Mission/Business Process Level); [SP 800-64]; [SP 800-160-1] (System Requirements Definition Process); [NIST CSF] (Core [Identify Function]; Profiles); [OMB FEA].

SYSTEM REGISTRATION

TASK P-17 Register the system with organizational program or management offices.

Potential Inputs: Organizational policy on system registration; system information.

Potential Outputs: Registered system in accordance with organizational policy.

Primary Responsibility: System Owner.

Supporting Role: Mission or Business Owner; Chief Information Officer; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: System registration, in accordance with organizational policy, serves to inform the governing organization of plans to develop the system or the existence of the system; the key characteristics of the system; and the expected security and privacy implications for the organization due to the operation and use of the system. System registration provides organizations with a management and tracking tool to facilitate bringing the system into the enterprise architecture, implementation of protections that are commensurate with risk, and security and privacy posture reporting in accordance with applicable laws, executive orders, directives, regulations, policies, or standards. As part of the system registration process, organizations add the system to the organization-wide system inventory. System registration information is updated with system categorization and system characterization information upon completion of the *Categorize* step.

References: None.

3.2 CATEGORIZE [67]

Purpose

The purpose of the ***Categorize*** step is to inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the Nation with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems.

CATEGORIZE TASKS

Table 3 provides a summary of tasks and expected outcomes for the RMF *Categorize* step. Applicable Cybersecurity Framework constructs are also provided.

TABLE 3: CATEGORIZE TASKS AND OUTCOMES

Tasks	Outcomes
TASK C-1 SECURITY CATEGORIZATION	• A security categorization of the system, including the information processed by the system represented by the organization-identified information types, is completed. [*Cybersecurity Framework*: **ID.AM-5**] • Security categorization results are documented in the security and privacy plans. [*Cybersecurity Framework*: **Profile**] • Security categorization results are consistent with the enterprise architecture and commitment to protecting organizational missions, business functions, and mission/business processes. • Security categorization results reflect the organization's risk management strategy.
TASK C-2 SECURITY CATEGORIZATION REVIEW AND APPROVAL	• The security categorization results are reviewed and the categorization decision is approved by senior leaders in the organization.
TASK C-3 SYSTEM DESCRIPTION	• The characteristics of the system are described and documented. [*Cybersecurity Framework*: **Profile**]

Quick link to summary table for RMF tasks, responsibilities, and supporting roles.

SECURITY CATEGORIZATION

TASK C-1 Categorize the system and document the security categorization results.

Potential Inputs: Risk management strategy; organizational risk tolerance; authorization boundary (i.e., system) information; organization- and system-level risk assessment results; information types processed,

[67] The RMF *Categorize* step is a precondition for the selection of security controls. However, for privacy, there are other factors considered by organizations that guide and inform the selection of privacy controls. These factors are described in the RMF *Prepare-System Level* step, Task P-15.

stored, or transmitted by the system; list of security and privacy requirements allocated to the system, system elements, and environment of operation; business impact analyses or criticality analyses.

Potential Outputs: Impact levels determined for each information type and for each security objective (confidentiality, integrity, availability); system categorization based on high water mark of information type impact levels.

Primary Responsibility: System Owner; Information Owner or Steward.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Authorizing Official or Authorizing Official Designated Representative; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Security categorization determinations consider potential adverse impacts to organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the loss of confidentiality, integrity, or availability of information. The categorization process is carried out by the system owner and the information owner or steward in cooperation and collaboration with senior leaders and executives with mission, business function, or risk management responsibilities. This ensures that individual systems are categorized based on the mission and business objectives of the organization. The system owner and information owner or steward consider the results from the security risk assessment (and the privacy risk assessment when the system processes PII) as a part of the security categorization decision. The decision is consistent with the risk management strategy. The results of the categorization process influence the selection of security controls for the system. Security categorization information is documented in the security plan or included as an attachment to the plan and can be cross-referenced in a privacy plan when the system processes PII.

The security categorization results for the system can be further refined by the organization to facilitate an impact-level prioritization of systems with the same impact level (see Task P-6). Results from the impact-level prioritization conducted by the organization can be used to help system owners in control selection and tailoring decisions.

References: [FIPS 199]; [SP 800-30]; [SP 800-39] (System Level); [SP 800-59]; [SP 800-60-1]; [SP 800-60-2]; [SP 800-160-1] (Stakeholder Needs and Requirements Definition and System Requirements Definition Processes); [IR 8179]; [CNSSI 1253]; [NIST CSF] (Core [Identify Function]).

SECURITY CATEGORIZATION REVIEW AND APPROVAL

TASK C-2 Review and approve the security categorization results and decision.

Potential Inputs: Impact levels determined for each information type and for each security objective (confidentiality, integrity, availability); system categorization based on high water mark of information type impact levels; list of high-value assets for the organization.

Potential Outputs: Approval of security categorization for the system.

Primary Responsibility: Authorizing Official or Authorizing Official Designated Representative; Senior Agency Official for Privacy.[68]

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; Senior Agency Information Security Officer.

[68] The senior agency official for privacy participates in determining whether the information processed by the information system is considered PII, and is involved in reviewing and approving the categorization for such systems.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: For information systems that process PII, the senior agency official for privacy reviews and approves the security categorization results and decision prior to the authorizing official's review.[69] Security categorization results and decisions are reviewed by the authorizing official or a designated representative to ensure that the security category selected for the information system is consistent with the mission and business functions of the organization and the need to adequately protect those missions and functions. The authorizing official or designated representatives reviews the categorization results and decision from an organization-wide perspective, including how the decision aligns with categorization decisions for all other organizational systems. The authorizing official collaborates with the senior agency official for risk management or the risk executive (function) to ensure that the categorization decision for the system is consistent with the organizational risk management strategy and satisfies requirements for high-value assets. As part of the approval process, the authorizing official can provide specific guidance to the system owner with respect to any limitations on baseline tailoring activities for the system that occur at the RMF *Select* step, Task S-3. If the security categorization decision is not approved, the system owner initiates steps to repeat the categorization process and resubmits the adjusted results to the authorizing official or designated representative. System registration information is subsequently updated with the approved security categorization information (see Task P-17).

References: [FIPS 199]; [SP 800-30]; [SP 800-39] (Organization Level); [SP 800-160-1] (Stakeholder Needs and Requirements Definition Process); [CNSSI 1253]; [NIST CSF] (Core [Identify Function]).

SYSTEM DESCRIPTION

TASK C-3 Document the characteristics of the system.

Potential Inputs: System design and requirements documentation; authorization boundary information; list of security and privacy requirements allocated to the system, system elements, and the environment of operation; system element information; system component inventory; system element supply chain information, including inventory and supplier information; system categorization; data map of the information life cycle for PII; information on system use, users, and roles.

Potential Outputs: Documented system description.

Primary Responsibility: System Owner.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Information Owner or Steward; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: A description of the system characteristics is documented in the security and privacy plans, included in attachments to the plans, or referenced in other standard sources for the information generated as part of the SDLC. Duplication of information is avoided, whenever possible. The level of detail in the security and privacy plans is determined by the organization and is commensurate with the security categorization and the security and privacy risk assessments of the system. Information may be added to the system description as it becomes available during the system life cycle and execution of the RMF steps.

Examples of different types of descriptive information that organizations can include in security and privacy plans include: descriptive name of the system and system identifier; system version or release number; manufacturer and supplier information; individual responsible for the system; system contact information; organization that manages, owns, or controls the system; system location; purpose of the

[69] The responsibilities of the senior agency official for privacy are detailed in [OMB A-130].

system and missions/business processes supported; how the system is integrated into the enterprise architecture; SDLC phase; results of the categorization process and privacy risk assessment; authorization boundary; laws, directives, policies, regulations, or standards affecting individuals' privacy and the security of the system; architectural description of the system including network topology; information types; hardware, firmware, and software components that are part of the system; hardware, software, and system interfaces (internal and external); information flows within the system; network connection rules for communicating with external systems; interconnected systems and identifiers for those systems; system users (including affiliations, access rights, privileges, citizenship); system provenance in the supply chain; maintenance or other relevant agreements; potential suppliers for replacement components for the system; alternative compatible system components; number and location in inventory of replacement system components; ownership or operation of the system (government-owned, government-operated; government-owned, contractor-operated; contractor-owned, contractor-operated; nonfederal [state and local governments, grantees]); incident response points of contact; authorization date and authorization termination date; and ongoing authorization status. System registration information is updated with the system characterization information (see Task P-17).

References: [SP 800-18]; [NIST CSF] (Core [Identify Function]).

3.3 SELECT

Purpose

The purpose of the ***Select*** step is to select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation.

SELECT TASKS

Table 4 provides a summary of tasks and expected outcomes for the RMF *Select* step. Applicable Cybersecurity Framework constructs are also provided.

TABLE 4: SELECT TASKS AND OUTCOMES

Tasks	Outcomes
TASK S-1 REQUIREMENTS ALLOCATION	• Security and privacy requirements are allocated to the system and to the environment in which the system operates. [*Cybersecurity Framework*: **ID.GV**]
TASK S-2 CONTROL SELECTION	• Control baselines necessary to protect the system commensurate with risk are selected. [*Cybersecurity Framework*: **Profile**] • Controls are assigned as system-specific, hybrid, or common controls. [*Cybersecurity Framework*: **Profile**; **PR.IP**]
TASK S-3 CONTROL TAILORING	• Controls are tailored producing tailored control baselines. [*Cybersecurity Framework*: **Profile**]
TASK S-4 PLAN DEVELOPMENT	• Controls and associated tailoring actions are documented in security and privacy plans or equivalent documents. [*Cybersecurity Framework*: **Profile**]
TASK S-5 CONTINUOUS MONITORING STRATEGY—SYSTEM	• A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed. [*Cybersecurity Framework*: **ID.GV**; **DE.CM**]
TASK S-6 PLAN REVIEW AND APPROVAL	• Security and privacy plans reflecting the selection of controls necessary to protect the system and the environment of operation commensurate with risk are reviewed and approved by the authorizing official.

Quick link to summary table for RMF tasks, responsibilities, and supporting roles.

REQUIREMENTS ALLOCATION

TASK S-1 Allocate security and privacy requirements to the information system and to the environment of operation.

Potential Inputs: System categorization; organization- and system-level risk assessment results; organizational policy on system registration; documented stakeholder protection needs; security and privacy requirements; list of common control providers and common controls available for inheritance;

system description; system element information; system component inventory; relevant laws, executive orders, directives, regulations, and policies.

Potential Outputs: List of security and privacy requirements allocated to the system, system elements, and the environment of operation.

Primary Responsibility: Security Architect; Privacy Architect; System Security Officer; System Privacy Officer.

Supporting Roles: Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative; Mission or Business Owner; Senior Agency Information Security Officer; Senior Agency Official for Privacy; System Owner.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: Organizations allocate security and privacy requirements to facilitate the control selection and implementation processes at the organization, information system, and system element (i.e., component) levels. The allocation of security and privacy requirements to the system and to the environment[70] in which the system operates, determines which controls are designated as system-specific, common, and hybrid during the control selection process. Requirements allocation also identifies the system elements (i.e., components) to which controls are assigned. The allocation of requirements conserves resources and facilitates streamlining of the risk management process by ensuring that requirements are not implemented on multiple systems or multiple components within a system when implementation of a common control or a system-level control on a specific component provides the needed protection capability. Common controls satisfy security and privacy requirements allocated to the organization and provide a protection capability that is inherited by one or more systems (see RMF *Prepare-Organization Level* step, Task P-5). Hybrid controls satisfy security and privacy requirements allocated to the system and to the organization and provide a protection capability that is partially inherited by one or more systems. And finally, system-specific controls satisfy security and privacy requirements allocated to the system and provide a protection capability for that system. Requirements can also be allocated to specific system components rather than to every component within a system. For example, system-specific controls associated with management of audit logs may be allocated to a log management server and thus need not be implemented on every system component.

References: [SP 800-39] (Organization, Mission/Business Process, and System Levels); [SP 800-64]; [SP 800-160-1] (System Requirements Definition Process); [NIST CSF] (Core [Identify Function]; Profiles); [OMB FEA].

CONTROL SELECTION

TASK S-2 Select the controls for the system and the environment of operation.

Potential Inputs: System categorization information; organization- and system-level risk assessment results; system element information; system component inventory; list of security and privacy requirements allocated to the system, system elements, and environment of operation; list of contractual requirements allocated to external providers of the system or system component; business impact or criticality analysis; risk management strategy; organizational security and privacy policy; federal or organization-approved or mandated baselines or overlays; Cybersecurity Framework profiles.

Potential Outputs: Controls selected for the system and the environment of operation.

[70] The environment of operation for an information system refers to the physical surroundings in which the system processes, stores, and transmits information. For example, *security requirements* are allocated to the facilities where the system is located and operates. Those security requirements can be satisfied by the physical security controls in [SP 800-53]

Primary Responsibility: System Owner; Common Control Provider.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Information Owner or Steward; Systems Security Engineer; Privacy Engineer; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Development/Acquisition.
Existing – Operations/Maintenance.

Discussion: There are two approaches that can be used for the initial selection of controls: a *baseline* control selection approach, or an *organization-generated* control selection approach. The baseline control selection approach uses control baselines, which are pre-defined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Control baselines serve as a starting point for the protection of individuals' privacy, information, and information systems. Federal control baselines are provided in [SP 800-53B]. The system security categorization (see Task C-1) and the security requirements derived from stakeholder protection needs, laws, executive orders, regulations, policies, directives, instructions, and standards (see Task P-15) can help inform the selection of security control baselines. A privacy risk assessment (see Task P-14) and privacy requirements derived from stakeholder protection needs, laws, executive orders, regulations, policies, directives, instructions, and standards (see Task P-15) can help inform the selection of privacy control baselines. Privacy programs use security and privacy control baselines to manage the privacy risks arising from both unauthorized system activity or behavior, as well as from authorized activities. After the pre-defined control baseline is selected, organizations tailor the baseline in accordance with the guidance provided (see Task S-3). The baseline control selection approach can provide consistency across a broad community of interest.

The organization-generated control selection approach differs from the baseline selection approach because the organization does not start with a pre-defined set of controls. Rather, the organization uses its own selection process to select controls. This may be necessary when the system is highly specialized (e.g., a weapons system or a medical device) or has limited purpose or scope (e.g., a smart meter). In these situations, it may be more efficient and cost-effective for an organization to select a specific set of controls for the system (i.e., a bottom-up approach) instead of starting with a pre-defined set of controls from a broad-based control baseline and subsequently eliminating controls through the tailoring process (i.e., top-down approach).

In both the baseline control selection approach and organization-generated control selection approach, organizations develop a well-defined set of security and privacy requirements using a life cycle-based systems engineering process (e.g., [ISO 15288] and [SP 800-160-1] as described in the RMF *Prepare-System Level* step, Task P-15. This process generates a set of requirements that can be used to guide and inform the selection of a set of controls to satisfy the requirements (whether the organization starts with a control baseline or generates the set of controls from its own selection process). Similarly, organizations can use the [NIST CSF] to develop *profiles* representing a set of organization-specific security and privacy requirements—and thus, guiding and informing control selection from [SP 800-53]. Tailoring may also be required in the organization-generated control selection approach (see Task S-3). Organizations do not need to choose one approach for the selection of controls for each of their systems, but instead, may use different approaches as circumstances dictate.

References: [FIPS 199]; [FIPS 200]; [SP 800-30]; [SP 800-53]; [SP 800-53B]; [SP 800-160-1] (System Requirements Definition, Architecture Definition, and Design Definition Processes); [SP 800-161] (Respond and Chapter 3); [IR 8062]; [IR 8179]; [CNSSI 1253]; [NIST CSF] (Core [Identify, Protect, Detect, Respond, Recover Functions]; Profiles).

CONTROL TAILORING

TASK S-3 Tailor the controls selected for the system and the environment of operation.

Potential Inputs: Initial control baselines; organization- and system-level risk assessment results; system element information; system component inventory; list of security and privacy requirements allocated to the system, system elements, and environment of operation; business impact analysis or criticality analysis; risk management strategy; organizational security and privacy policies; federal or organization-approved or mandated overlays.

Potential Outputs: List of tailored controls for the system and environment of operation (i.e., tailored control baselines).

Primary Responsibility: System Owner; Common Control Provider.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Information Owner or Steward; Systems Security Engineer; Privacy Engineer; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Development/Acquisition.
Existing – Operations/Maintenance.

Discussion: After selecting the applicable control baselines, organizations tailor the controls based on various factors including, for example, missions or business functions, threats, privacy risks, supply chain risks, type of system, or risk tolerance. Controls related to SCRM provide the basis for determining whether an information system is fit-for-purpose[71] and need to be tailored accordingly. The tailoring process includes identifying and designating common controls in the control baselines (see Task P-5); applying scoping considerations to the remaining baseline controls; selecting compensating controls, if needed; assigning specific values to organization-defined control parameters using either assignment or selection statements; supplementing baselines with additional controls; and providing specification information for control implementation.[72] Organizations determine the amount of detail to include in justifications or supporting rationale required for tailoring decisions. For example, the justification or supporting rationale for scoping decisions related to a high-impact system (or high value asset) may necessitate greater specificity than similar decisions for a low-impact system. Such determinations are consistent with the organization's missions and business functions; stakeholder needs; and any relevant laws, executive orders, regulations, directives, or policies.

Organizations use risk assessments to inform and guide the tailoring process. Threat information from security risk assessments provides information on adversary capabilities, intent, and targeting that may affect organizational decisions regarding the selection of security controls, including the associated costs and benefits. Privacy risk assessments, including the contextual factors therein, will also influence tailoring when an information system processes PII.[73] Risk assessment results are also leveraged when identifying common controls to determine if the controls available for inheritance meet the security and privacy requirements for the system and its environment of operation. When common controls provided by the organization are not sufficient for the systems inheriting the controls, system owners can either supplement the common controls with system-specific or hybrid controls to achieve the required level of protection for the system or accept greater risk with the acknowledgement and approval of the organization. Organizations may also consider federally or organizationally mandated or approved overlays, tailored baselines, or Cybersecurity Framework Profiles when conducting tailoring (see Task P-4).

References: [FIPS 199]; [FIPS 200]; [SP 800-30]; [SP 800-53]; [SP 800-53B]; [SP 800-160-1] (System Requirements Definition, Architecture Definition, and Design Definition Processes); [SP 800-161] (Respond and Chapter 3); [IR 8179]; [CNSSI 1253]; [NIST CSF] (Core [Identify, Protect, Detect, Respond, Recover Functions]; Profiles).

[71] [ISO 15288] describes *fit-for-purpose* as an outcome from the validation process in the SDLC that demonstrates, through assessment of the services presented to the stakeholders, that the "right" system has been created and satisfies the customer need.

[72] The tailoring process is fully described in [SP 800-53B].

[73] [IR 8062] provides a discussion of context and its function in a privacy risk model.

PLAN DEVELOPMENT

TASK S-4 Document the controls for the system and environment of operation in security and privacy plans.

Potential Inputs: System categorization information; organization- and system-level risk assessment results; system element information; system component inventory; business impact or criticality analysis; list of security and privacy requirements allocated to the system, system elements, and environment of operation; risk management strategy; list of selected controls for the system and environment of operation; organizational security and privacy policies.

Potential Outputs: Security and privacy plans for the system.

Primary Responsibility: System Owner; Common Control Provider.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Information Owner or Steward; Systems Security Engineer; Privacy Engineer; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Development/Acquisition.
Existing – Operations/Maintenance.

Discussion: Security and privacy plans contain an overview of the security and privacy requirements for the system and the controls selected to satisfy the requirements. The plans describe the intended application of each selected control in the context of the system with a sufficient level of detail to correctly implement the control and to subsequently assess the effectiveness of the control. The control documentation describes how system-specific and hybrid controls are implemented and the plans and expectations regarding the functionality of the system. The description includes planned inputs, expected behavior, and expected outputs where appropriate, typically for those controls implemented in the hardware, software, or firmware components of the system. Common controls are also identified in the plans. There is no requirement to provide implementation details for inherited common controls. Rather, those details are provided in the plans for common control providers and are made available to system owners. For hybrid controls, the organization specifies in the system-level plans the parts of the control that are provided by the common control provider and the parts of the control that are implemented at the system level.

Organizations may develop a consolidated plan that incorporates security and privacy plans, or maintain separate plans. Privacy programs collaborate on the development of the security component of an integrated plan in the following areas. When controls provide protections with respect to managing confidentiality, integrity, and availability of PII, privacy programs collaborate with security programs to ensure that the plan reflects the selection of these controls and delineates roles and responsibilities for control implementation, assessment, and monitoring. For separate security plans and privacy plans, organizations cross-reference the controls in all plans to help to maintain awareness and accountability. The senior agency official for privacy reviews and approves the privacy plan (or integrated plan) before the plan is provided to the authorizing official or designated representative for review (see Task S-6). Organizations may document control selection and tailoring information in documents equivalent to security and privacy plans, for example, in systems engineering or system life cycle artifacts or documents.

Documentation of planned control implementations allows for traceability of decisions prior to and after the deployment of the system. To the extent possible, organizations reference existing documentation (either by vendors or other organizations that have employed the same or similar systems or system elements), use automated support tools, and coordinate across the organization to reduce redundancy and increase the efficiency and cost-effectiveness of control documentation. The documentation also addresses platform dependencies and includes any additional information necessary to describe how the capability required is to be achieved at the level of detail sufficient to support control implementation and assessment. Documentation for control implementations follows best practices for hardware and software development and for systems security and privacy engineering disciplines and is also consistent with established policies and procedures for documenting activities in the SDLC. In certain situations, security controls can be implemented in ways that create privacy risks. The privacy program supports documentation of privacy risk considerations and the implementations intended to mitigate them.

For controls that are mechanism-based, organizations take advantage of the functional specifications provided by or obtainable from manufacturers, vendors, and systems integrators. This includes any documentation that may assist the organization during the development, implementation, assessment, and monitoring of controls. For certain controls, organizations obtain control implementation information from the appropriate organizational entities including, for example, physical security offices, facilities offices, records management offices, and human resource offices. Since the enterprise architecture and the security and privacy architectures established by the organization guide and inform the organizational approach used to plan for and implement controls, documenting the process helps to ensure traceability in meeting the security and privacy requirements.

References: [FIPS 199]; [FIPS 200]; [SP 800-18]; [SP 800-30]; [SP 800-53]; [SP 800-64]; [SP 800-160-1] (System Requirements Definition, Architecture Definition, and Design Definition Processes); [SP 800-161] (Respond and Chapter 3); [IR 8179]; [CNSSI 1253]; [NIST CSF] (Core [Identify, Protect, Detect, Respond, Recover Functions]; Profiles).

CONTINUOUS MONITORING STRATEGY—SYSTEM

TASK S-5 Develop and implement a system-level strategy for monitoring control effectiveness to supplement the organizational continuous monitoring strategy.

Potential Inputs: Organizational risk management strategy; organizational continuous monitoring strategy; organization- and system-level risk assessment results; security and privacy plans; organizational security and privacy policies.

Potential Outputs: Continuous monitoring strategy for the system including time-based trigger for ongoing authorization.

Primary Responsibility: System Owner; Common Control Provider.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Authorizing Official or Authorizing Official Designated Representative; Information Owner or Steward; Security Architect; Privacy Architect; Systems Security Engineer; Privacy Engineer; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Development/Acquisition.
Existing – Operations/Maintenance.

Discussion: An important aspect of risk management is the ongoing monitoring of controls implemented within or inherited by an information system. An effective continuous monitoring strategy at the system level is developed and implemented in coordination with the organizational continuous monitoring strategy early in the SDLC (i.e., during initial system design or procurement decision). The system-level continuous monitoring strategy supplements the continuous monitoring strategy for the organization. The system-level strategy addresses monitoring those controls for which monitoring is not provided as part of the continuous monitoring strategy and implementation for the organization. The system-level strategy identifies the frequency of monitoring for controls not addressed by the organization-level strategy and defines the approach to be used for assessing those controls. The system-level continuous monitoring strategy, consistent with the organizational strategy, may define how changes to the system are to be monitored; how risk assessments are to be conducted; and the security and privacy posture reporting requirements including recipients of the reports. The system-level continuous monitoring strategy can be included in security and privacy plans.[74]

For controls that are not addressed by the organizational continuous monitoring strategy, the criteria for determining the frequency with which controls are monitored post-implementation and a plan for the ongoing assessment of those controls, are established by the system owner or common control provider in collaboration with other organizational officials including, for example, the authorizing official or designated representative; senior accountable official for risk management or risk executive (function); senior agency information security officer; senior agency official for privacy; and chief information officer. The frequency criteria at the system level reflect organizational priorities and the importance of the system to the organization's operations and assets, individuals, other organizations, and the Nation. Controls that are volatile (i.e., where the control or the control implementation is most likely to change over time),[75] critical to certain aspects of the protection needs for the organization, or identified in plans of action and milestones, may require more frequent assessment. The approach to control assessments during continuous monitoring may include, for example, reuse of assessment procedures and assessment results that supported the initial authorization decision; detection of the status of system components; and analysis of historical and operational data.

The authorizing official or designated representative approves the continuous monitoring strategy and the minimum frequency with which each control is to be monitored. The approval of the strategy can be obtained in conjunction with the security and privacy plan approval. The monitoring of controls begins at the start of the operational phase of the SDLC and continues through the disposal phase.

References: [SP 800-30]; [SP 800-39] (Organization, Mission or Business Process, System Levels); [SP 800-53]; [SP 800-53A]; [SP 800-137]; [SP 800-161]; [IR 8011-1]; [CNSSI 1253]; [NIST CSF] (Core [Detect Function]).

PLAN REVIEW AND APPROVAL

TASK S-6 Review and approve the security and privacy plans for the system and the environment of operation.

Potential Inputs: Completed security and privacy plans; organization- and system-level risk assessment results.

Potential Outputs: Security and privacy plans approved by the authorizing official.

Primary Responsibility: Authorizing Official or Authorizing Official Designated Representative.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; Chief Acquisition Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

[74] The Privacy Continuous Monitoring (PCM) strategy includes all of the available privacy controls implemented throughout the organization at all risk management levels (i.e., organization, mission/business process, and system). The strategy ensures that the controls are monitored on an ongoing basis by assigning an organization-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. If, during the development of a new system, there is a need to create or use a privacy control not included in the PCM strategy, the SAOP is consulted to determine whether it is appropriate for the proposed use case. If there is a decision to implement a new privacy control, the organization's PCM strategy is updated to include the new control with an organization-defined monitoring frequency.

[75] Volatility is most prevalent in those controls implemented in the hardware, software and firmware components of the system. For example, replacing or upgrading an operating system, a database system, application, or a network router may change the security controls provided by the vendor or original equipment manufacturer. Moreover, configuration settings may also require adjustments as organizational missions, business functions, threats, risks, and risk tolerance change.

System Development Life Cycle Phase: New – Development/Acquisition.
Existing – Operations/Maintenance.

Discussion: The security and privacy plan review by the authorizing official or designated representative with support from the senior accountable official for risk management or risk executive (function), chief information officer, senior agency information security officer, and senior agency official for privacy, determines if the plans are complete, consistent, and satisfy the stated security and privacy requirements for the system. Based on the results from this review, the authorizing official or designated representative may recommend changes to the security and privacy plans. If the plans are unacceptable, the system owner or common control provider make appropriate changes to the plans. If the plans are acceptable, the authorizing official or designated representative approves the plans.

The acceptance of the security and privacy plans represents an important milestone in the SDLC and risk management process. The authorizing official or designated representative, by approving the plans, agrees to the set of controls (i.e., system-specific, hybrid, or common controls) and the description of the proposed implementation of the controls to meet the security and privacy requirements for the system and the environment in which the system operates. The approval of the plans allows the risk management process to proceed to the RMF *Implement* step. The approval of the plans also establishes the level of effort required to successfully complete the remainder of the RMF steps and provides the basis of the security and privacy specifications for the acquisition of the system or individual system components.

References: [SP 800-30]; [SP 800-53]; [SP 800-160-1] (System Requirements Definition, Architecture Definition, and Design Definition Processes).

3.4 IMPLEMENT

Purpose

The purpose of the ***Implement*** step is to implement the controls in the security and privacy plans for the system and for the organization and to document in a baseline configuration, the specific details of the control implementation.

IMPLEMENT TASKS

Table 5 provides a summary of tasks and expected outcomes for the RMF *Implement* step. Applicable Cybersecurity Framework constructs are also provided.

TABLE 5: IMPLEMENT TASKS AND OUTCOMES

Tasks	Outcomes
TASK I-1 CONTROL IMPLEMENTATION	• Controls specified in the security and privacy plans are implemented. [*Cybersecurity Framework*: **PR.IP-1**] • Systems security and privacy engineering methodologies are used to implement the controls in the system security and privacy plans. [*Cybersecurity Framework*: **PR.IP-2**]
TASK I-2 BASELINE CONFIGURATION	• The configuration baseline is established. [*Cybersecurity Framework*: **PR.IP-1**] • The security and privacy plans are updated based on information obtained during the implementation of the controls. [*Cybersecurity Framework*: **Profile**]

Quick link to summary table for RMF tasks, responsibilities, and supporting roles.

CONTROL IMPLEMENTATION

TASK I-1 Implement the controls in the security and privacy plans.

Potential Inputs: Approved security and privacy plans; system design documents; organizational security and privacy policies and procedures; business impact or criticality analyses; enterprise architecture information; security architecture information; privacy architecture information; list of security and privacy requirements allocated to the system, system elements; and environment of operation; system element information; system component inventory; organization- and system-level risk assessment results.

Potential Outputs: Implemented controls.

Primary Responsibility: System Owner; Common Control Provider.

Supporting Roles: Information Owner or Steward; Security Architect; Privacy Architect; Systems Security Engineer; Privacy Engineer; System Security Officer; System Privacy Officer; Enterprise Architect; System Administrator.

System Development Life Cycle Phase: New – Development/Acquisition; Implementation/Assessment.
Existing – Operations/Maintenance.

Discussion: Organizations implement the controls listed in the security and privacy plans. The control implementation is consistent with the organization's enterprise architecture and associated security and privacy architectures. The security and privacy architectures serve as a resource to guide and inform the allocation of controls to a system or system component. Not all controls need to be allocated to every system component. Controls providing a specific security or privacy capability are only allocated to system components that require that capability. The security categorization, privacy risk assessment, security and privacy architectures, and the allocation of controls work together to help achieve a suitable balance between security and privacy protections and the mission-based function of the system.

Organizations use best practices when implementing controls, including systems security and privacy engineering methodologies, concepts, and principles. Risk assessments guide and inform decisions regarding the cost, benefit, and risk trade-offs in using different technologies or policies for control implementation. Organizations also ensure that mandatory configuration settings are established and implemented on system components in accordance with federal and organizational policies. When organizations have no direct control over what controls are implemented in a system component, for example, in commercial off-the-shelf products, organizations consider the use of system components that have been tested, evaluated, or validated by approved, independent, third-party assessment facilities (e.g., NIST Cryptographic Module Validation Program Testing Laboratories, National Information Assurance Partnership Common Criteria Testing Laboratories). In addition, organizations address, where applicable, assurance requirements when implementing controls. Assurance requirements are directed at the activities that control developers and implementers carry out to increase the level of confidence that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system. The assurance requirements address quality of the design, development, and implementation of the controls.[76]

For the common controls inherited by the system, systems security and privacy engineers with support from system security and privacy officers, coordinate with the common control provider to determine the most appropriate way to implement common controls. System owners can refer to the authorization packages prepared by common control providers when making determinations regarding the adequacy of common controls inherited by their systems. During implementation, it may be determined that common controls previously selected to be inherited by the system do not meet the specified security or privacy requirements for the system. For common controls that do not meet the requirements for the system inheriting the controls or when common controls have unacceptable deficiencies, the system owners identify compensating or supplementary controls to be implemented. System owners can supplement the common controls with system-specific or hybrid controls to achieve the required protection for their systems or they can accept greater risk with the acknowledgement and approval of the organization. Risk assessments may determine how gaps in security or privacy requirements between systems and common controls affect the risk associated with the system, and how to prioritize the need for compensating or supplementary controls to mitigate specific risks.

Consistent with the flexibility allowed in applying the tasks in the RMF, organizations conduct initial control assessments during system development and implementation. Conducting such assessments in parallel with the development and implementation phases of the SDLC facilitates early identification of deficiencies and provides a cost-effective method for initiating corrective actions. Issues discovered during these assessments can be referred to authorizing officials for resolution. The results of the initial control assessments can also be used during the authorize step to avoid delays or costly repetition of assessments. Assessment results that are subsequently reused in other phases of the SDLC meet the reuse requirements established by the organization.[77]

[76] [SP 800-53] provides a list of assurance-related security and privacy controls.

[77] See the RMF *Assess* step and [SP 800-53A] for information on assessments and reuse of assessment results.

References: [FIPS 200]; [SP 800-30]; [SP 800-53]; [SP 800-53A]; [SP 800-160-1] (Implementation, Integration, Verification, and Transition Processes); [SP 800-161]; [IR 8062]; [IR 8179].

BASELINE CONFIGURATION

TASK I-2 Establish the initial configuration baseline for the system by documenting changes to planned control implementation.

Potential Inputs: Security and privacy plans; information from control implementation efforts.

Potential Outputs: Security and privacy plans updated with implementation detail sufficient for use by assessors; system configuration baseline.

Primary Responsibility: System Owner; Common Control Provider.

Supporting Roles: Information Owner or Steward; Security Architect; Privacy Architect; Systems Security Engineer; Privacy Engineer; System Security Officer; System Privacy Officer; Enterprise Architect; System Administrator.

System Development Life Cycle Phase: New – Development/Acquisition; Implementation/Assessment.
Existing – Operations/Maintenance.

Discussion: Despite the specific control implementation details in the security and privacy plans and the system design documents, it is not always feasible to implement controls as planned. Therefore, as control implementations are carried out, the security and privacy plans are updated with as-implemented control implementation details. The updates include revised descriptions of implemented controls including changes to planned inputs, expected behavior, and expected outputs with sufficient detail to support control assessments. Configuration baselines are established for all aspects of the information system including any information technology component (i.e., hardware, software, and firmware) configurations and include system configuration settings and other technical implementation details. The configuration baselines are essential to providing the capability to determine when there are changes to the system, whether those changes are authorized, and the impact of the changes on the security and privacy posture of the system and the organization.

References: [SP 800-53]; [SP 800-128]; [SP 800-160-1] (Implementation, Integration, Verification, and Transition, Configuration Management Processes).

3.5 ASSESS

Purpose

The purpose of the ***Assess*** step is to determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization.

ASSESS TASKS

Table 6 provides a summary of tasks and expected outcomes for the RMF *Assess* step. Applicable Cybersecurity Framework constructs are also provided.

TABLE 6: ASSESS TASKS AND OUTCOMES

Tasks	Outcomes
TASK A-1 ASSESSOR SELECTION	- An assessor or assessment team is selected to conduct the control assessments. - The appropriate level of independence is achieved for the assessor or assessment team selected.
TASK A-2 ASSESSMENT PLAN	- Documentation needed to conduct the assessments is provided to the assessor or assessment team. - Security and privacy assessment plans are developed and documented. - Security and privacy assessment plans are reviewed and approved to establish the expectations for the control assessments and the level of effort required.
TASK A-3 CONTROL ASSESSMENTS	- Control assessments are conducted in accordance with the security and privacy assessment plans. - Opportunities to reuse assessment results from previous assessments to make the risk management process timely and cost-effective are considered. - Use of automation to conduct control assessments is maximized to increase speed, effectiveness, and efficiency of assessments.
TASK A-4 ASSESSMENT REPORTS	- Security and privacy assessment reports that provide findings and recommendations are completed.
TASK A-5 REMEDIATION ACTIONS	- Remediation actions to address deficiencies in the controls implemented in the system and environment of operation are taken. - Security and privacy plans are updated to reflect control implementation changes made based on the assessments and subsequent remediation actions. [*Cybersecurity Framework*: **Profile**]
TASK A-6 PLAN OF ACTION AND MILESTONES	- A plan of action and milestones detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed. [*Cybersecurity Framework*: **ID.RA-6**]

Quick link to summary table for RMF tasks, responsibilities, and supporting roles.

ASSESSOR SELECTION

TASK A-1 Select the appropriate assessor or assessment team for the type of control assessment to be conducted.

Potential Inputs: Security and privacy plans; program management control information; common control documentation; organizational security and privacy program plans; system design documentation; enterprise, security, and privacy architecture information; security and privacy policies and procedures applicable to the system.

Potential Outputs: Selection of assessor or assessment team responsible for conducting the control assessment.

Primary Responsibility: Authorizing Official or Authorizing Official Designated Representative.

Supporting Roles: Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

System Development Life Cycle Phase: New – Development/Acquisition; Implementation/Assessment.
Existing – Operations/Maintenance.

Discussion: Organizations consider both the technical expertise and level of independence required in selecting control assessors.[78] Organizations ensure that control assessors possess the required skills and technical expertise to develop effective assessment plans and to conduct assessments of program management, system-specific, hybrid, and common controls, as appropriate. This includes general knowledge of risk management concepts as well as comprehensive knowledge of and experience with the specific hardware, software, and firmware components implemented. As controls may be implemented to achieve security and privacy objectives, organizations consider the degree of collaboration between security control and privacy control assessors that is necessary.

Organizations can conduct self-assessments of controls or obtain the services of an independent control assessor. An independent assessor is an individual or group that is capable of conducting an impartial assessment. Impartiality means that assessors are free from perceived or actual conflicts of interest with respect to the determination of control effectiveness or the development, operation, or management of the system, common controls, or program management controls. The authorizing official determines the level of assessor independence based on applicable laws, executive orders, directives, regulations, policies, or standards. The authorizing official consults with the Office of the Inspector General, chief information officer, senior agency official for privacy, and senior agency information security officer to help guide and inform decisions regarding assessor independence.

The system privacy officer is responsible for identifying assessment methodologies and metrics to determine if privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks. The senior agency official for privacy is also responsible for conducting assessments of privacy controls and documenting the results of the assessments. At the discretion of the organization, privacy controls may be assessed by an independent assessor. However, in all cases, the senior agency official for privacy is responsible and accountable for the organization's privacy program, including any privacy functions performed by independent assessors. The senior agency official for privacy is also responsible for providing privacy-related information to the authorizing official.

References: [FIPS 199]; [SP 800-30]; [SP 800-53A]; [SP 800-55].

[78] In accordance with [OMB A-130], an independent evaluation of privacy program and practices is not required. However, an organization may choose to employ independent privacy assessments at the organization's discretion.

ASSESSMENT PLAN

TASK A-2 Develop, review, and approve plans to assess implemented controls.

Potential Inputs: Security and privacy plans; program management control information; common control documentation; organizational security and privacy program plans; system design documentation; enterprise, security, and privacy architecture information; policies and procedures applicable to the system.

Potential Outputs: Security and privacy assessment plans approved by the authorizing official.

Primary Responsibility: Authorizing Official or Authorizing Official Designated Representative; Control Assessor.

Supporting Roles: Senior Agency Information Security Officer; Senior Agency Official for Privacy; System Owner; Common Control Provider; Information Owner or Steward; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Development/Acquisition; Implementation/Assessment.
Existing – Operations/Maintenance.

Discussion: Security and privacy assessment plans are developed by control assessors based on the implementation information contained in security and privacy plans, program management control documentation, and common control documentation. Organizations may choose to develop a single, integrated security and privacy assessment plan for the system or the organization. An integrated assessment plan delineates roles and responsibilities for control assessment. Assessment plans also provide the objectives for control assessments and specific assessment procedures for each control. Assessment plans reflect the type of assessment the organization is conducting, including for example: developmental testing and evaluation; independent verification and validation; audits, including supply chain; assessments supporting system and common control authorization or reauthorization; program management control assessments; continuous monitoring; and assessments conducted after remediation actions.

Assessment plans are reviewed and approved by the authorizing official or the designated representative of the authorizing official to help ensure that the plans are consistent with the security and privacy objectives of the organization; employ procedures, methods, techniques, tools, and automation to support continuous monitoring and near real-time risk management; and are cost-effective. Approved assessment plans establish expectations for the control assessments and the level of effort for the assessment. Approved assessment plans help to ensure that appropriate resources are applied toward determining control effectiveness while providing the necessary level of assurance in making such determinations. When controls are provided by an external provider through contracts, interagency agreements, lines of business arrangements, licensing agreements, or supply chain arrangements, the organization can request security and privacy assessment plans and assessments results or evidence from the provider.

References: [SP 800-53A]; [SP 800-160-1] (Verification and Validation Processes); [SP 800-161]; [IR 8011-1].

CONTROL ASSESSMENTS

TASK A-3 Assess the controls in accordance with the assessment procedures described in assessment plans.

Potential Inputs: Security and privacy assessment plans; security and privacy plans; external assessment or audit results (if applicable).

Potential Outputs: Completed control assessments and associated assessment evidence.

Primary Responsibility: Control Assessor.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; System Owner; Common Control Provider; Information Owner or Steward; Senior Agency Information Security Officer; Senior Agency Official for Privacy; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Development/Acquisition; Implementation/Assessment.
Existing – Operations/Maintenance.

Discussion: Control assessments determine the extent to which the selected controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security and privacy requirements for the system and the organization. The system owner, common control provider, and/or organization rely on the technical skills and expertise of assessors to assess implemented controls using the assessment procedures specified in assessment plans and provide recommendations on how to respond to control deficiencies to reduce or eliminate identified vulnerabilities or unacceptable risks. The senior agency official for privacy serves as the control assessor for the privacy controls and is responsible for conducting an initial assessment of the privacy controls prior to system operation, and for assessing the controls periodically thereafter at a frequency sufficient to ensure compliance with privacy requirements and to manage privacy risks.[79] Controls implemented to achieve both security and privacy objectives may require a degree of collaboration between security and privacy control assessors. The assessor findings are a factual reporting of whether the controls are operating as intended and whether any deficiencies[80] in the controls are discovered during the assessment.

Control assessments occur as early as practicable in the SDLC, preferably during the development phase. These types of assessments are referred to as developmental testing and evaluation and validate that the controls are implemented correctly and are consistent with the established information security and privacy architectures. Developmental testing and evaluation activities include, for example, design and code reviews, regression testing, and application scanning. Deficiencies identified early in the SDLC can be resolved in a more cost-effective manner. Assessments may be needed prior to source selection during the procurement process to assess potential suppliers or providers before the organization enters into agreements or contracts to begin the development phase. The results of control assessments conducted during the SDLC can also be used (consistent with reuse criteria established by the organization) during the authorization process to avoid unnecessary delays or costly repetition of assessments. Organizations can maximize the use of automation to conduct control assessments to increase the speed, effectiveness, and efficiency of the assessments, and to support continuous monitoring of the security and privacy posture of organizational systems.

Applying and assessing controls throughout the development process may be appropriate for iterative development processes. When iterative development processes (e.g., agile development) are employed, an iterative assessment may be conducted as each cycle is completed. A similar process is employed for assessing controls in commercial IT products that are used in the system. Organizations may choose to begin assessing controls prior to the complete implementation of all controls in the security and privacy plans. This type of incremental assessment is appropriate if it is more efficient or cost-effective to do so. Common controls (i.e., controls that are inherited by the system) are assessed separately (by assessors chosen by common control providers or the organization) and need not be assessed as part of a system-level assessment.

Organizations ensure that assessors have access to the information system and environment of operation where the controls are implemented and to the documentation, records, artifacts, test results, and other materials needed to assess the controls. This includes the controls implemented by external providers through contracts, interagency agreements, lines of business arrangements, licensing agreements, or supply chain arrangements. Assessors have the required degree of independence as determined by the

[79] The senior agency official for privacy can delegate the assessment functions, consistent with applicable policies.

[80] Only deficiencies in controls that can be exploited by threat agents are considered vulnerabilities.

authorizing official.[81] Assessor independence during the continuous monitoring process facilitates reuse of assessment results to support ongoing authorization and reauthorization.

To make the risk management process more efficient and cost-effective, organizations may choose to establish reasonable and appropriate criteria for reusing assessment results as part of organization-wide assessment policy or in the security and privacy program plans. For example, a recent audit of a system may have produced information about the effectiveness of selected controls. Another opportunity to reuse previous assessment results may come from external programs that test and evaluate security and privacy features of commercial information technology products (e.g., Common Criteria Evaluation and Validation Program and NIST Cryptographic Module Validation Program,). If prior assessment results from the system developer or vendor are available, the control assessor, under appropriate circumstances, may incorporate those results into the assessment. In addition, if a control implementation was assessed during other forms of assessment at previous stages of the SDLC (e.g., unit testing, functional testing, acceptance testing), organizations may consider potential reuse of those results to reduce duplication of efforts. And finally, assessment results can be reused to support reciprocity, for example, assessment results supporting an authorization to use (see Appendix F). Additional information on assessment result reuse is available in [SP 800-53A].

References: [SP 800-53A]; [SP 800-160-1] (Verification and Validation Processes); [IR 8011-1].

ASSESSMENT REPORTS

TASK A-4 Prepare the assessment reports documenting the findings and recommendations from the control assessments.

Potential Inputs: Completed control assessments[82] and associated assessment evidence.

Potential Outputs: Completed security and privacy assessment reports detailing the assessor findings and recommendations.

Primary Responsibility: Control Assessor.

Supporting Roles: System Owner; Common Control Provider; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Development/Acquisition; Implementation/Assessment.
Existing – Operations/Maintenance.

Discussion: The results of the security and privacy control assessments, including recommendations for correcting deficiencies in the implemented controls, are documented in the assessment reports[83] by control assessors. Organizations may develop a single, integrated security and privacy assessment report. Assessment reports are key documents in the system or common control authorization package that is developed for authorizing officials. The assessment reports include information based on assessor findings, necessary to determine the effectiveness of the controls implemented within or inherited by the information system. Assessment reports are an important factor in a determining risk to organizational operations and assets, individuals, other organizations, and the Nation by the authorizing official. The format and the level of detail provided in assessment reports are appropriate for the type of control assessment conducted, for example, developmental testing and evaluation; independent verification and

[81] In accordance with [OMB A-130], an independent evaluation of privacy program and practices is not required. However, an organization may choose to employ independent privacy assessments at the organization's discretion.

[82] A *privacy control assessment* is defined in [OMB A-130] as both an assessment and a formal document detailing the process and the outcome of the assessment. In this guideline, a privacy assessment report is identified as a separate output, but it should be considered as part of the privacy control assessment.

[83] If a comparable report meets the requirements of what is to be included in an assessment report, then the comparable report would itself constitute the assessment report.

validation; independent assessments supporting information system or common control authorizations or reauthorizations; self-assessments; assessments after remediation actions; independent evaluations or audits; and assessments during continuous monitoring. The reporting format may also be prescribed by the organization.

Control assessment results obtained during the system development lifecycle are documented in an interim report and included in the final security and privacy assessment reports. Development of interim reports that document assessment results from relevant phases of the SDLC reinforces the concept that assessment reports are evolving documents. Interim reports are used, as appropriate, to inform the final assessment report. Organizations may choose to develop an executive summary from the control assessment findings. The executive summary provides authorizing officials and other interested individuals in the organization with an abbreviated version of the assessment reports that includes a synopsis of the assessment, findings, and the recommendations for addressing deficiencies in the controls.

References: [SP 800-53A]; [SP 800-160-1] (Verification and Validation Processes).

REMEDIATION ACTIONS

TASK A-5 Conduct initial remediation actions on the controls and reassess remediated controls.

Potential Inputs: Completed security and privacy assessment reports with findings and recommendations; security and privacy plans; security and privacy assessment plans; organization- and system-level risk assessment results.

Potential Outputs: Completed initial remediation actions based on the security and privacy assessment reports; changes to implementations reassessed by the assessment team; updated security and privacy assessment reports; updated security and privacy plans including changes to the control implementations.

Primary Responsibility: System Owner; Common Control Provider; Control Assessor.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Senior Accountable Official for Risk Management or Risk Executive (Function); System Owner; Information Owner or Steward; Systems Security Engineer; Privacy Engineer; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Development/Acquisition; Implementation/Assessment.
Existing – Operations/Maintenance.

Discussion: The security and privacy assessment reports describe deficiencies in the controls implemented within the system or the common controls available for inheritance that could not be resolved during the development of the system or that are discovered post-development. Such control deficiencies may result in security, privacy, and supply chain risks. The findings generated during control assessments provide information that facilitates a disciplined and structured approach to responding to those risks in accordance with the organizational risk tolerance and priorities. Findings from a system-level control assessment may necessitate an update to the system risk assessment and the organizational risk assessment.[84] The updated risk assessment and any inputs from the senior accountable official for risk management or risk executive (function) determines the initial remediation actions and the prioritization of those actions. System owners and common control providers may decide, based on a risk assessment, that certain findings are inconsequential and present no significant security or privacy risk. Such findings are retained in the security and privacy assessment reports and monitored during the monitoring step. The authorizing official is responsible for reviewing and understanding the assessor findings and for

[84] Risk assessments are conducted as needed at the organizational level, mission/business level, and at the system level throughout the SDLC. Risk assessment is specified as part of the RMF *Prepare-Organization Level* step, Task P-3 and RMF *Prepare-System Level* step, Task P-14.

accepting the security, privacy, and supply chain risks from operating an information system or the use of common controls. The authorizing official, in consultation with system owners and other organizational officials, may decide that certain findings do, in fact, represent significant, unacceptable risk and require immediate remediation actions.

In all cases, organizations review assessor findings to determine the significance of the findings (i.e., the potential adverse impact on organizational operations and assets, individuals, other organizations, or the Nation) and whether the findings warrant any further investigation or remediation. Senior leadership involvement in the mitigation process is necessary to help ensure that the organization's resources are effectively allocated in accordance with organizational priorities, providing resources to the systems that are supporting the most critical missions and business functions or correcting the deficiencies that pose the greatest risk. If deficiencies in controls are corrected, the assessors reassess the remediated controls. Control reassessments determine the extent to which remediated controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization. The assessors update the assessment reports with the findings from the reassessment, but do not change the original assessment results. The security and privacy plans are updated based on the findings of the control assessments and any remediation actions taken. The updated plans reflect the state of the controls after the initial assessment and any modifications by the system owner or common control provider in addressing recommendations for corrective actions. At the completion of the control assessments, security and privacy plans contain an accurate description of implemented controls, including compensating controls.

Organizations can prepare an addendum to the security and privacy assessment reports that provides an opportunity for system owners and common control providers to respond to initial assessment findings. The addendum may include, for example, information regarding initial remediation actions taken by system owners or common control providers in response to assessor findings. The addendum can also provide the system owner or common control provider perspective on the findings. This may include providing additional explanatory material, rebutting certain findings, and correcting the record. The addendum does not change or influence the initial assessor findings provided in the reports. Information provided in the addendum is considered by authorizing officials when making risk-based authorization decisions. Organizations implement a process to determine the actions to take regarding the control deficiencies identified during the assessment. This process can address vulnerabilities and risks, false positives, and other factors that provide useful information to authorizing officials regarding the security and privacy posture of the system and organization including the ongoing effectiveness of system-specific, hybrid, and common controls. The issue resolution process can also ensure that only substantive items are identified and transferred to the plan of actions and milestones.

References: [SP 800-53A]; [SP 800-160-1] (Verification and Validation Processes).

PLAN OF ACTION AND MILESTONES

TASK A-6 Prepare the plan of action and milestones based on the findings and recommendations of the assessment reports.

Potential Inputs: Updated security and privacy assessment reports; updated security and privacy plans; organization- and system-level risk assessment results; organizational risk management strategy and risk tolerance.

Potential Outputs: A plan of action and milestones detailing the findings from the security and privacy assessment reports that are to be remediated.

Primary Responsibility: System Owner; Common Control Provider.

Supporting Roles: Information Owner or Steward; System Security Officer; System Privacy Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Chief Acquisition Officer.

System Development Life Cycle Phase: New – Implementation/Assessment.
Existing – Operations/Maintenance.

Discussion: The plan of action and milestones, prepared for the authorizing official by the system owner or the common control provider, is included as part of the authorization package. It describes the actions that are planned to correct deficiencies in the controls identified during the assessment of the controls and during continuous monitoring. The plan of action and milestones includes tasks to be accomplished with a recommendation for completion before or after system authorization; resources required to accomplish the tasks; milestones established to meet the tasks; and the scheduled completion dates for the milestones and tasks. The plan of action and milestones is reviewed by the authorizing official to ensure there is agreement with the remediation actions planned to correct the identified deficiencies. It is subsequently used to monitor progress in completing the actions. Deficiencies are accepted by the authorizing official as residual risk or are remediated during the assessment or prior to submission of the authorization package to the authorizing official. Plan of action and milestones entries are not necessary when deficiencies are accepted by the authorizing official as residual risk. However, deficiencies identified during assessment and monitoring are documented in the assessment reports, which can be retained within an automated security/privacy management and reporting tool to maintain an effective audit trail. Organizations develop plans of action and milestones based on assessment results obtained from control assessments, audits, and continuous monitoring and in accordance with applicable laws, executive orders, directives, policies, regulations, standards, or guidance.

Organizations implement a consistent process for developing plans of action and milestones that uses a prioritized approach to risk mitigation that is uniform across the organization. A risk assessment guides the prioritization process for items included in the plan of action and milestones. The process ensures that plans of action and milestones are informed by the security categorization of the system and security, privacy, and supply chain risk assessments; the specific deficiencies in the controls; the criticality of the identified control deficiencies (i.e., the direct or indirect effect that the deficiencies may have on the security and privacy posture of the system, and therefore, on the risk exposure of the organization; or the ability of the organization to perform its mission or business functions); and the proposed risk mitigation approach to address the identified deficiencies in the controls, including, for example, prioritization of risk mitigation actions and allocation of risk mitigation resources. Risk mitigation resources include, for example, personnel, new hardware or software, and tools.

References: [SP 800-30]; [SP 800-53A]; [SP 800-160-1] (Verification and Validation Processes); [IR 8062].

3.6 AUTHORIZE

Purpose

The purpose of the *Authorize* step is to provide organizational accountability by requiring a senior management official to determine if the security, privacy, and supply chain risk to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system or the use of common controls, is acceptable.

AUTHORIZE TASKS

Table 7 provides a summary of tasks and expected outcomes for the RMF *Authorize* step. Applicable Cybersecurity Framework constructs are also provided.

TABLE 7: AUTHORIZE TASKS AND OUTCOMES

Tasks	Outcomes
TASK R-1 AUTHORIZATION PACKAGE	• An authorization package is developed for submission to the authorizing official.
TASK R-2 RISK ANALYSIS AND DETERMINATION	• A risk determination by the authorizing official that reflects the risk management strategy including risk tolerance, is rendered.
TASK R-3 RISK RESPONSE	• Risk responses for determined risks are provided. [*Cybersecurity Framework*: **ID.RA-6**]
TASK R-4 AUTHORIZATION DECISION	• The authorization for the system or the common controls is approved or denied.
TASK R-5 AUTHORIZATION REPORTING	• Authorization decisions, significant vulnerabilities, and risks are reported to organizational officials.

Quick link to summary table for RMF tasks, responsibilities, and supporting roles.

AUTHORIZATION PACKAGE

TASK R-1 Assemble the authorization package and submit the package to the authorizing official for an authorization decision.

Potential Inputs: Security and privacy plans; security and privacy assessment reports; plan of action and milestones; supporting assessment evidence or other documentation, as required.

Potential Outputs: Authorization package (with an executive summary), which may be generated from a security or privacy management tool[85] for submission to the authorizing official.

Primary Responsibility: System Owner; Common Control Provider; Senior Agency Official for Privacy.[86]

[85] Organizations are encouraged to maximize the use of automated tools in the preparation, assembly, and transmission of authorization packages and security- and privacy-related information supporting the authorization process. Many commercially available governance, risk, and compliance (GRC) tools can be employed to reduce or eliminate hard copy documentation.

[86] The senior agency official for privacy is active for information systems processing PII.

Supporting Roles: System Security Officer; System Privacy Officer; Senior Agency Information Security Officer; Control Assessor.

System Development Life Cycle Phase: New – Implementation/Assessment.
Existing – Operations/Maintenance.

Discussion: Authorization packages[87] include security and privacy plans, security and privacy assessment reports, plans of action and milestones, and an executive summary. Additional information can be included in the authorization package at the request of the authorizing official. Organizations maintain version and change control as the information in the authorization package is updated. Providing timely updates to the plans, assessment reports, and plans of action and milestones on an ongoing basis supports the concept of near real-time risk management and ongoing authorization, and can be used for reauthorization actions, if required.

The senior agency official for privacy reviews the authorization package for systems that process PII to ensure compliance with applicable privacy requirements and to manage privacy risks, prior to authorizing officials making risk determination and acceptance decisions.

The information in the authorization package is used by authorizing officials to make informed, risk-based decisions. When controls are implemented by an external provider through contracts, interagency agreements, lines of business arrangements, licensing agreements, or supply chain arrangements, the organization ensures that the information needed to make risk-based decisions is made available by the provider.

The authorization package may be provided to the authorizing official in hard copy or electronically or may be generated using an automated security/privacy management and reporting tool. Organizations can use automated support tools in preparing and managing the content of the authorization package. Such tools provide an effective vehicle for maintaining and updating information for authorizing officials regarding the ongoing security and privacy posture of information systems within the organization.

When an information system is under ongoing authorization, the authorization package is presented to the authorizing official via automated reports to provide information in the most efficient and timely manner possible.[88] Information to be presented to the authorizing official in assessment reports is generated in the format and with the frequency determined by the organization using information from the information security and privacy continuous monitoring programs.

The assessment reports presented to the authorizing official include information about implemented system-specific, hybrid, and common controls. The authorizing official uses automated security/privacy management and reporting tools or other automated methods, whenever practicable, to access the security and privacy plans and the plans of action and milestones. The authorization documents are updated at an organization-defined frequency using automated or manual processes in accordance with the risk management objectives of the organization.[89]

References: [SP 800-18]; [SP 800-160-1] (Risk Management Process); [SP 800-161] (SCRM Plans).

[87] If a comparable report meets the requirements of what is to be included in an authorization package, then the comparable report would itself constitute the authorization package.

[88] While the objective is to fully automate all components of the authorization package, organizations may be in various states of transition to a fully automated state—that is, with certain sections of the authorization package available via automated means and other sections available only through manual means.

[89] Organizations decide on the level of detail and the presentation format of security and privacy information that is made available to authorizing officials through automation. These decisions are based on organizational needs with the automated presentation of security- and privacy-related information tailored to the decision-making needs of the authorizing officials. For example, detailed security- and privacy-related information may be generated and collected at the operational level of the organization with information subsequently analyzed, distilled, and presented to authorizing officials in a summarized or highlighted format using automation.

RISK ANALYSIS AND DETERMINATION

TASK R-2 Analyze and determine the risk from the operation or use of the system or the provision of common controls.

Potential Inputs: Authorization package; supporting assessment evidence or other documentation as required; information provided by the senior accountable official for risk management or risk executive (function); organizational risk management strategy and risk tolerance; organization- and system-level risk assessment results.

Potential Outputs: Risk determination.

Primary Responsibility: Authorizing Official or Authorizing Official Designated Representative.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Information Security Officer; Senior Agency Official for Privacy.

System Development Life Cycle Phase: New – Implementation/Assessment.
Existing – Operations/Maintenance.

Discussion: The authorizing official or designated representative, in collaboration with the senior agency information security officer and the senior agency official for privacy (for information systems processing PII), analyzes the information in the authorization package provided by the control assessor, system owner, or common control provider, and finalizes the determination of risk. Further discussion with the control assessor, system owner, or common control provider may be necessary to help ensure a thorough understanding of risk by the authorizing official.

Risk assessments are employed, if needed, to provide information[90] that may influence the risk analysis and determination. The senior accountable official for risk management or risk executive (function) may provide information to the authorizing official that is considered in the final determination of risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from either the operation or use of the system or the provision of common controls. Such information may include, for example, organizational risk tolerance, dependencies among systems and controls, mission and business requirements, the criticality of the missions or business functions supported by the system, or the risk management strategy.

The authorizing official analyzes the information provided by the senior accountable official for risk management or risk executive (function) and information provided by the system owner or common control provider in the authorization package when making a risk determination. The information provided by the senior accountable official for risk management or risk executive (function) is documented and included, to the extent it is relevant, as part of the authorization decision (see Task R-4). The authorizing official may also use an automated security/privacy management and reporting tool to annotate senior accountable official for risk management or risk executive (function) input.

When the system is operating under an ongoing authorization, the risk determination task is effectively unchanged. The authorizing official analyzes the relevant security and privacy information provided by the automated security/privacy management and reporting tool to determine the current security and privacy posture of the system.

References: [SP 800-30]; [SP 800-39] (Organization, Mission/Business Process, and System Levels); [SP 800-137]; [SP 800-160-1] (Risk Management Process); [IR 8062].

[90] [SP 800-30] provides guidance on conducting security risk assessments. [IR 8062] provides information about privacy risk assessments and associated risk factors.

RISK RESPONSE

TASK R-3 Identify and implement a preferred course of action in response to the risk determined.

Potential Inputs: Authorization package; risk determination; organization- and system-level risk assessment results.

Potential Outputs: Risk responses for determined risks.

Primary Responsibility: Authorizing Official or Authorizing Official Designated Representative.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Information Security Officer; Senior Agency Official for Privacy; System Owner or Common Control Provider; Information Owner or Steward; Systems Security Engineer; Privacy Engineer; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Implementation/Assessment.
Existing – Operations/Maintenance.

Discussion: After risk is analyzed and determined, organizations can respond to risk in a variety of ways, including acceptance of risk and mitigation of risk. Existing risk assessment results and risk assessment techniques may be used to help determine the preferred course of action for the risk response.[91] When the response to risk is mitigation, the planned mitigation actions are included in and tracked using the plan of action and milestones. When the response to risk is acceptance, the deficiency found during the assessment process remains documented in the security and privacy assessment reports and is monitored for changes to the risk factors.[92] Because the authorizing official is the only person who can accept risk, the authorizing official is responsible for reviewing the assessment reports and plans of action and milestones and determining whether the identified risks need to be mitigated prior to authorization. Decisions on the most appropriate course of action for responding to risk may include some form of prioritization. Some risks may be of greater concern to organizations than other risks. In that case, more resources may need to be directed at addressing higher-priority risks versus lower-priority risks. This does not necessarily mean that the lower-priority risks are ignored. Rather, it could mean that fewer resources are directed at addressing the lower-priority risks, or that the lower-priority risks are addressed later. A key part of the risk-based decision process is the recognition that regardless of the risk response, there remains a degree of residual risk. Organizations determine acceptable degrees of residual risk based on organizational risk tolerance.

References: [SP 800-30]; [SP 800-39] (Organization, Mission/Business Process, and System Levels); [SP 800-160-1] (Risk Management Process); [IR 8062]; [IR 8179]; [NIST CSF] (Core [Identify Function]).

AUTHORIZATION DECISION

TASK R-4 Determine if the risk from the operation or use of the information system or the provision or use of common controls is acceptable.

Potential Inputs: Risk responses for determined risks.

Potential Outputs: Authorization to operate, authorization to use, common control authorization; denial of authorization to operate, denial of authorization to use, denial of common control authorization.

Primary Responsibility: Authorizing Official.

[91] [SP 800-39] provides additional information on risk response.

[92] The four security risk factors are threat, vulnerability, likelihood, and impact. [SP 800-30] and [SP 800-39] provide information about security risk assessments and associated risk factors. [IR 8062] and Section 2.3 provide additional information on privacy risk factors and conducting privacy risk assessments.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Information Security Officer; Senior Agency Official for Privacy; Authorizing Official Designated Representative.

System Development Life Cycle Phase: New – Implementation/Assessment.
Existing – Operations/Maintenance.

Discussion: The explicit acceptance of risk is the responsibility of the authorizing official and cannot be delegated to other officials within the organization. The authorizing official considers many factors when deciding if the risk to the organization's operations (including mission, functions, image, and reputation) and assets, individuals, other organizations, or the Nation, is acceptable. Balancing security and privacy considerations with mission and business needs is paramount to achieving an acceptable risk-based authorization decision.[93] The authorizing official issues an authorization decision for the system or for organization-designated common controls after reviewing the information in the authorization package, input from other organizational officials (see Task R-2), and other relevant information that may affect the authorization decision. The authorization package provides the most current information on the security and privacy posture of the system or the common controls.

The authorization decision is conveyed by the authorizing official to the system owner or common control provider, and other organizational officials, as appropriate.[94] The authorization decision also conveys the terms and conditions for the authorization to operate; the authorization termination date or time-driven authorization frequency; input from the senior accountable official for risk management or risk executive (function), if provided; and for common control authorizations, the system impact level supported by the common controls.

For systems, the authorization decision indicates to the system owner whether the system is authorized to operate or authorized to use, or not authorized to operate or not authorized to use. For common controls, the authorization decision indicates to the common control provider and to the system owners of inheriting systems, whether the common controls are authorized to be provided or not authorized to be provided. The terms and conditions for the common control authorization provide a description of any specific limitations or restrictions placed on the operation of the system or the controls that must be followed by the system owner or common control provider.

The authorization termination date is established by the authorizing official and indicates when the authorization expires. Organizations may eliminate the authorization termination date if the system is operating under an ongoing authorization—that is, the continuous monitoring program is sufficiently robust and mature to provide the authorizing official with the needed information to conduct ongoing risk determination and risk acceptance activities regarding the security and privacy posture of the system and the ongoing effectiveness of the controls employed within and inherited by the system.

The authorization decision is included with the authorization package and is transmitted to the system owner or common control provider. Upon receipt of the authorization decision and the authorization package, the system owner or common control provider acknowledges and implements the terms and conditions of the authorization. The organization ensures that the authorization package, including the authorization decision for systems and common controls, is made available to organizational officials

[93] While balancing security and privacy considerations with mission and business needs is paramount to achieving an acceptable risk-based authorization decision, there may be instances when the authorizing official and senior agency official for privacy cannot reach a final resolution regarding the appropriate protection for PII and the information systems that process PII. [OMB A-130] provides guidance on how to resolve such instances.

[94] Organizations are encouraged to employ automated security/privacy management and reporting tools whenever feasible, to develop the authorization packages for systems and common controls and to maintain those packages during ongoing authorization. Automated tools can significantly reduce documentation costs, provide increased speed and efficiency in generating important information for decision makers, and provide more effective means for updating critical risk management information. It is recognized that certain controls are not conducive to the use of automated tools and therefore, manual methods are acceptable in those situations.

including, for example, system owners inheriting common controls; chief information officers; senior accountable officials for risk management or risk executive (function); senior agency information security officers; senior agency officials for privacy; and system security and privacy officers. The authorizing official verifies on an ongoing basis as part of continuous monitoring (see Task M-2) that the established terms and conditions for authorization are being followed by the system owner or common control provider.

When the system is operating under ongoing authorization, the authorizing official continues to be responsible and accountable for explicitly understanding and accepting the risk of continuing to operate or use the system or continuing to provide common controls for inheritance. For ongoing authorization, the authorization frequency is specified in lieu of an authorization termination date. The authorizing official reviews the information with the specific time-driven authorization frequency defined by the organization as part of the continuous monitoring strategy and determines if the risk of continued system operation or the provision of common controls remains acceptable. If the risk remains acceptable, the authorizing official acknowledges the acceptance in accordance with organizational processes. If not, the authorizing official indicates that the risk is no longer acceptable and requires further risk response or a full denial of the authorization.

The organization determines the level of formality for the process of communicating and acknowledging continued risk acceptance by the authorizing official. The authorizing official may continue to establish and convey the specific terms and conditions to be followed by the system owner or common control provider for continued authorization to operate, continued common control authorization, or continued authorization to use. The terms and conditions of the authorization may be conveyed through an automated management and reporting tool as part of an automated authorization decision.

If control assessments are conducted by qualified assessors with the level of independence[95] required, the assessment results support ongoing authorization and may be applied to a reauthorization. Organizational policies regarding ongoing authorization and reauthorization are consistent with laws, executive orders, directives, regulations, and policies.

The authorizing official consults with the Senior Accountable Official for Risk Management or the Risk Executive (Function) prior to making the final authorization decision for the information system or the common controls. Because there are potentially significant dependencies among organizational systems and with external systems, the authorization decisions for individual systems consider the current residual risk, organizational plans of action and milestones, and the risk tolerance of the organization.

Appendix F provides additional guidance on authorization decisions, the types of authorizations, and the preparation of the authorization packages.

References: [SP 800-39] (Organization, Mission/Business Process, and System Levels); [SP 800-160-1] (Risk Management Process).

AUTHORIZATION REPORTING

TASK R-5 Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk.

Potential Inputs: Authorization decision.

Potential Outputs: A report indicating the authorization decision for a system or set of common controls; annotation of authorization status in the organizational system registry.

Primary Responsibility: Authorizing Official or Authorizing Official Designated Representative.

[95] In accordance with [OMB A-130], an independent evaluation of privacy program and practices is not required. However, an organization may choose to employ independent privacy assessments at the organization's discretion.

Supporting Roles: System Owner or Common Control Provider; Information Owner or Steward; System Security Officer; System Privacy Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

System Development Life Cycle Phase: New – Implementation/Assessment.
Existing – Operations/Maintenance.

Discussion: Authorizing officials report authorization decisions for systems and common controls to designated organizational officials so the individual risk decisions can be viewed in the context of organization-wide security and privacy risk to organizational operations and assets, individuals, other organizations, and the Nation. Reporting occurs only in situations where organizations have delegated the authorization functions to levels of the organization below the head of agency. Authorizing officials also report exploitable deficiencies (i.e., vulnerabilities) in the system or controls noted during the assessment and continuous monitoring that represent significant security or privacy risk. Organizations determine, and the organizational policy reflects, what constitutes a significant security or privacy risk for reporting. Deficiencies that represent significant vulnerabilities and risk can be reported using the subcategories, categories, and functions in the [NIST CSF]. Authorization decisions may be tracked and reflected as part of the organization-wide system registration process at the organization's discretion (see Task P-17).

References: [SP 800-39] (Organization, Mission/Business Process, and System Levels); [SP 800-160-1] (Decision Management and Project Assessment and Control Processes); [NIST CSF] (Core [Identify, Protect, Detect, Respond, Recover Functions]).

3.7 MONITOR

Purpose

The purpose of the ***Monitor*** step is to maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions.

MONITOR TASKS

Table 8 provides a summary of tasks and expected outcomes for the RMF *Monitor* step. Applicable Cybersecurity Framework constructs are also provided.

TABLE 8: MONITOR TASKS AND OUTCOMES

Tasks	Outcomes
TASK M-1 SYSTEM AND ENVIRONMENT CHANGES	• The information system and environment of operation are monitored in accordance with the continuous monitoring strategy. [*Cybersecurity Framework*: **DE.CM**; **ID.GV**]
TASK M-2 ONGOING ASSESSMENTS	• Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy. [*Cybersecurity Framework*: **ID.SC-4**]
TASK M-3 ONGOING RISK RESPONSE	• The output of continuous monitoring activities is analyzed and responded to appropriately. [*Cybersecurity Framework*: **RS.AN**]
TASK M-4 AUTHORIZATION UPDATES	• Risk management documents are updated based on continuous monitoring activities. [*Cybersecurity Framework*: **RS.IM**]
TASK M-5 SECURITY AND PRIVACY REPORTING	• A process is in place to report the security and privacy posture to the authorizing official and other senior leaders and executives.
TASK M-6 ONGOING AUTHORIZATION	• Authorizing officials conduct ongoing authorizations using the results of continuous monitoring activities and communicate changes in risk determination and acceptance decisions.
TASK M-7 SYSTEM DISPOSAL	• A system disposal strategy is developed and implemented, as needed.

Quick link to summary table for RMF tasks, responsibilities, and supporting roles.

SYSTEM AND ENVIRONMENT CHANGES

TASK M-1 Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system.

Potential Inputs: Organizational continuous monitoring strategy; organizational configuration management policy and procedures; organizational policy and procedures for handling unauthorized system changes; security and privacy plans; configuration change requests/approvals; system design documentation; security and privacy assessment reports; plans of action and milestones; information from automated and manual monitoring tools.

Potential Outputs: Updated security and privacy plans; updated plans of action and milestones; updated security and privacy assessment reports.

Primary Responsibility: System Owner or Common Control Provider; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Authorizing Official or Authorizing Official Designated Representative; Information Owner or Steward; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Operations/Maintenance.
Existing – Operations/Maintenance.

Discussion: Systems and environments of operation are in a constant state of change with changes occurring in the technology or machine elements, human elements, and physical or environmental elements. Changes to the technology or machine elements include for example, upgrades to hardware, software, or firmware; changes to the human elements include for example, staff turnover or a reduction in force; and modifications to the surrounding physical and environmental elements include for example, changes in the location of the facility or the physical access controls protecting the facility. When changes are made by external providers, those changes can be difficult to detect. A disciplined and structured approach to managing, controlling, and documenting changes to systems and environments of operation, and adherence with terms and conditions of the authorization, is an essential element of security and privacy programs. Organizations establish configuration management and control processes to support configuration and change management.[96]

Common activities within organizations can cause changes to systems or the environments of operation and can have a significant impact on the security and privacy posture of systems. Examples include installing or disposing of hardware, making changes to configurations, and installing patches outside of the established configuration change control process. Unauthorized changes may occur because of purposeful attacks by adversaries or inadvertent errors by authorized personnel. In addition to adhering to the established configuration management process, organizations monitor for unauthorized changes to systems and analyze information about unauthorized changes that have occurred to determine the root cause of the unauthorized change. In addition to monitoring for unauthorized changes, organizations continuously monitor systems and environments of operation for any authorized changes that impact the privacy posture of systems.[97]

Once the root cause of an unauthorized change (or an authorized change that impacts the privacy posture of the system) has been determined, organizations respond accordingly (see Task M-3). For example, if the root cause of an unauthorized change is determined to be an adversarial attack, multiple actions could be taken such as invoking incident response processes, adjusting intrusion detection and prevention tools and firewall configurations, or implementing additional or stronger controls to reduce the risk of future attacks. If the root cause of an unauthorized change is determined to be a failure of staff to adhere to established configuration management processes, remedial training for certain individuals may be warranted.

References: [SP 800-30]; [SP 800-128]; [SP 800-137]; [IR 8062].

[96] [SP 800-128] provides guidance on security-focused configuration management (SecCM). Note that the SecCM process described in [SP 800-128] includes a related monitoring step.

[97] For information about the distinction between authorized and unauthorized system behavior, see the discussion of security and privacy in Section 2.3.

ONGOING ASSESSMENTS

Task M-2 Assess the controls implemented within and inherited by the system in accordance with the continuous monitoring strategy.

Potential Inputs: Organizational continuous monitoring strategy and system level continuous monitoring strategy (if applicable); security and privacy plans; security and privacy assessment plans; security and privacy assessment reports; plans of action and milestones; organization- and system-level risk assessment results; external assessment or audit results (if applicable); information from automated and manual monitoring tools.

Potential Outputs: Updated security and privacy assessment reports.

Primary Responsibility: Control Assessor.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; System Owner or Common Control Provider; Information Owner or Steward; System Security Officer; System Privacy Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

System Development Life Cycle Phase: New – Operations/Maintenance.
Existing – Operations/Maintenance.

Discussion: After an initial system or common control authorization, the organization assesses all controls implemented within and inherited by the system on an ongoing basis. This ongoing assessment of the effectiveness of controls is part of an organization's continuous monitoring activities. The monitoring frequency for each control is based on the organizational continuous monitoring strategy (see Task P-7) and can be supplemented by the system-level continuous monitoring strategy (see Task S-5). Adherence to the terms and conditions specified by the authorizing official as part of the authorization decision are also monitored (see Task M-1). Ongoing control assessment continues as the information generated as part of continuous monitoring is correlated, analyzed, and reported to senior leaders.

For ongoing control assessments, assessors have the required degree of independence as determined by the authorizing official.[98] Assessor independence during continuous monitoring introduces efficiencies into the process and may allow for reuse of assessment results in support of ongoing authorization and when reauthorization is required.

To satisfy the annual FISMA security assessment requirement, organizations can use assessment results from control assessments that occurred during authorization, ongoing authorization, or reauthorization; during continuous monitoring; or the during testing and evaluation of systems as part of the SDLC or an audit (provided the assessment results are current, relevant to the determination of control effectiveness, and obtained by assessors with the required degree of independence). Existing assessment results are reused consistent with the reuse policy established by the organization and are supplemented with additional assessments as needed. The reuse of assessment results is helpful in achieving a cost-effective, security program capable of producing the evidence necessary to determine the security posture of information systems and the organization. Finally, the use of automation to support control assessments facilitates a greater frequency, volume, and coverage of assessments.

References: [SP 800-53A]; [SP 800-137]; [SP 800-160-1] (Verification, Validation, Operation, and Maintenance Processes); [IR 8011-1].

ONGOING RISK RESPONSE

Task M-3 Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones.

[98] In accordance with [OMB A-130], an independent evaluation of privacy programs and practices is not required. However, an organization may choose to employ independent privacy assessments at the organization's discretion.

Potential Inputs: Security and privacy assessment reports; organization- and system-level risk assessment results; security and privacy plans; plans of action and milestones.

Potential Outputs: Mitigation actions or risk acceptance decisions; updated security and privacy assessment reports.

Primary Responsibility: Authorizing Official; System Owner; Common Control Provider.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Official for Privacy; Authorizing Official Designated Representative; Information Owner or Steward; System Security Officer; System Privacy Officer; Systems Security Engineer; Privacy Engineer; Security Architect; Privacy Architect.

System Development Life Cycle Phase: New – Operations/Maintenance.
Existing – Operations/Maintenance.

Discussion: Assessment information produced by an assessor during continuous monitoring is provided to the system owner and the common control provider in updated assessment reports or via reports from automated security/privacy management and reporting tools. The authorizing official determines the appropriate risk response to the assessment findings or approves responses proposed by the system owner and common control provider. The system owner and common control provider subsequently implement the appropriate risk response. When the risk response is acceptance, the findings remain documented in the security and privacy assessment reports and are monitored for changes to risk factors. When the risk response is mitigation, the planned mitigation actions are included in and tracked using the plans of action and milestones. If requested by the authorizing official, control assessors may provide recommendations for remediation actions. Recommendations for remediation actions may also be provided by an automated security/privacy management and reporting tool. An organizational assessment of risk (Task P-3) and system-level risk assessment results (Task P-14) guide and inform the decisions regarding ongoing risk response. Controls that are modified, enhanced, or added as part of ongoing risk response are reassessed by assessors to ensure that the new, modified, or enhanced controls have been implemented correctly, are operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements of the system.

References: [SP 800-30]; [SP 800-53]; [SP 800-53A]; [SP 800-137]; [SP 800-160-1] (Risk Management Process); [IR 8011-1]; [IR 8062]; [NIST CSF] (Core [Respond Functions]).

AUTHORIZATION UPDATES

Task M-4 Update plans, assessment reports, and plans of action and milestones based on the results of the continuous monitoring process.

Potential Inputs: Security and privacy assessment reports; organization- and system-level risk assessment results; security and privacy plans; plans of action and milestones.

Potential Outputs: Updated security and privacy assessment reports;[99] updated plans of action and milestones; updated risk assessment results; updated security and privacy plans.

Primary Responsibility: System Owner; Common Control Provider.

Supporting Roles: Information Owner or Steward; System Security Officer; System Privacy Officer; Senior Agency Official for Privacy; Senior Agency Information Security Officer.

System Development Life Cycle Phase: New – Operations/Maintenance.
Existing – Operations/Maintenance.

[99] If a comparable report meets the requirements of what is to be included in an assessment report (e.g., a report generated from a security or privacy management and reporting tool), then the comparable report would constitute the assessment report.

Discussion: To achieve near real-time risk management, the organization updates security and privacy plans, security and privacy assessment reports, and plans of action and milestones on an ongoing basis. Updates to the plans reflect modifications to controls based on risk mitigation activities carried out by system owners or common control providers. Updates to control assessment reports reflect additional assessment activities carried out to determine control effectiveness based on implementation details in the plans. Plans of action and milestones are updated based on progress made on the current outstanding items; address security and privacy risks discovered as part of control effectiveness monitoring; and describe how the system owner or common control provider intends to address those risks. The updated information raises awareness of the security and privacy posture of the system and the common controls inherited by the system, thereby, supporting near real-time risk management and the ongoing authorization process.

The frequency of updates to risk management-related information is at the discretion of the system owner, common control provider, and authorizing officials in accordance with federal and organizational policies and is consistent with the organizational and system-level continuous monitoring strategies. The updates to information regarding the security and privacy posture of the system and the common controls inherited by the system are accurate and timely since the information provided influences ongoing actions and decisions by authorizing officials and other senior leaders within the organization. The use of automated support tools and organization-wide security and privacy program management practices ensure that authorizing officials can readily access the current security and privacy posture of the system. This provides essential information for continuous monitoring and ongoing authorization and promotes the near real-time management of risk to organizational operations and assets, individuals, other organizations, and the Nation.

Organizations ensure that information needed for oversight, management, and auditing purposes is not modified or destroyed when updating security and privacy plans, assessment reports, and plans of action and milestones. Providing an effective method to track changes to systems through configuration management procedures is necessary to achieve transparency and traceability in the security and privacy activities of the organization; to obtain individual accountability for any security or privacy actions; and to understand emerging trends in the security and privacy programs of the organization.

References: [SP 800-53A].

POSTURE REPORTING

Task M-5 Report the security and privacy posture of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy.

Potential Inputs: Security and privacy assessment reports; plans of action and milestones; organization- and system-level risk assessment results; organization- and system-level continuous monitoring strategy; security and privacy plans; Cybersecurity Framework profile.

Potential Outputs: Security and privacy posture reports.[100]

Primary Responsibility: System Owner; Common Control Provider; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

Supporting Roles: System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Operations/Maintenance.
Existing – Operations/Maintenance.

[100] If a comparable report meets the requirements of what is to be included in a security or privacy posture report (e.g., a report generated from a security or privacy management and reporting tool), then the comparable report would constitute the posture report.

Discussion: The results of monitoring activities are documented and reported to the authorizing official and other selected organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy. Other organizational officials who may receive security and privacy posture reports include, for example, chief information officer, senior agency information security officer, senior agency official for privacy, senior agency official for risk management or risk executive (function), information owner or steward, incident response roles, and contingency planning roles. Security and privacy posture reporting can be event-driven, time-driven, or event- and time-driven.[101] The reports provide the authorizing official and other organizational officials with information regarding the security and privacy posture of the systems including the effectiveness of implemented controls. Security and privacy posture reports describe the ongoing monitoring activities employed by system owners or common control providers. The reports also include information about security and privacy risks in the systems and environments of operation discovered during control assessments, auditing, and continuous monitoring and how system owners or common control providers plan to address those risks.

Organizations have flexibility in the breadth, depth, formality, form, and format of security and privacy posture reports. The goal is efficient ongoing communication with the authorizing official and other organizational officials as necessary, conveying the current security and privacy posture of systems and environments of operation and how the current posture affects individuals, organizational missions, and business functions. At a minimum, security and privacy posture reports summarize changes to the security and privacy plans, security and privacy assessment reports, and plans of action and milestones that have occurred since the last report. The use of automated security and privacy management and reporting tools (e.g., a dashboard) by the organization facilitates the effectiveness and timeliness of security and privacy posture reporting.

The frequency of security and privacy posture reports is at the discretion of the organization and in compliance with federal and organizational policies. Reports occur at appropriate intervals to transmit security- and privacy-related information about systems or common controls but not so frequently as to generate unnecessary work or expense. Authorizing officials use the security and privacy posture reports and consult with the senior accountable official for risk management or risk executive (function), senior agency information security officer, and senior agency official for privacy to determine if a reauthorization action is necessary.

Security and privacy posture reports are marked, protected, and handled in accordance with federal and organizational policies. Security and privacy posture reports can be used to satisfy FISMA reporting requirements for documenting remediation actions for security- and privacy-related weaknesses or deficiencies. Such reporting is intended to be ongoing and should not be interpreted as requiring the time, expense, and formality associated with the information provided for the initial authorization. Rather, reporting is conducted in a cost-effective manner consistent with achieving the reporting objectives.

References: [SP 800-53A]; [SP 800-137]; [NIST CSF] (Core [Identify, Protect, Detect, Respond, Recover Functions]).

ONGOING AUTHORIZATION

Task M-6 Review the security and privacy posture of the system on an ongoing basis to determine whether the risk remains acceptable.

Potential Inputs: Risk tolerance; security and privacy posture reports; plans of action and milestones; organization- and system-level risk assessment results; security and privacy plans.

Potential Outputs: A determination of risk; ongoing authorization to operate, ongoing authorization to use, ongoing common control authorization; denial of ongoing authorization to operate, denial of ongoing authorization to use, denial of ongoing common control authorization.

[101] See Appendix F for more information about time- and event-driven authorizations and reporting.

Primary Responsibility: Authorizing Official.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Information Security Officer; Senior Agency Official for Privacy; Authorizing Official Designated Representative.

System Development Life Cycle Phase: New – Operations/Maintenance.
Existing – Operations/Maintenance.

Discussion: To employ an ongoing authorization approach, organizations have in place an organization-level and system-level continuous monitoring process to assess implemented controls on an ongoing basis. The findings or results from the continuous monitoring process provides useful information to authorization officials to support near-real time risk-based decision making. In accordance with the guidance in Task R-4, the authorizing official or designated representative reviews the security and privacy posture of the system (including the effectiveness of the implemented controls) on an ongoing basis to determine the current risk to organizational operations and assets, individuals, other organizations, and the Nation. The authorizing official determines whether the current risk is acceptable and provides appropriate direction to the system owner or common control provider.

The risks may change based on the information provided in the security and privacy posture reports because the reports may indicate changes to the security or privacy risk factors. Determining how changing conditions affect organizational and individual risk is essential for managing privacy risk and maintaining adequate security. By carrying out ongoing risk determination and risk acceptance, authorizing officials can maintain system and common control authorizations over time and transition to ongoing authorization. Reauthorization actions occur only in accordance with federal or organizational policies. The authorizing official conveys updated risk determination and acceptance results to the senior accountable official for risk management or the risk executive (function).

The use of automated support tools to capture, organize, quantify, visually display, and maintain security and privacy posture information promotes near real-time risk management regarding the risk posture of the organization. The use of metrics and dashboards increases an organization's capability to make risk-based decisions by consolidating data in an automated fashion and providing the data to decision makers at different levels within the organization in an easy-to-understand format.

References: [SP 800-30]; [SP 800-39] (Organization, Mission/Business Process, and System Levels); [SP 800-55]; [SP 800-160-1] (Risk Management Process); [IR 8011-1]; [IR 8062].

SYSTEM DISPOSAL

Task M-7 Implement a system disposal strategy and execute required actions when a system is removed from operation.

Potential Inputs: Security and privacy plans; organization- and system-level risk assessment results; system component inventory.

Potential Outputs: Disposal strategy; updated system component inventory; updated security and privacy plans.

Primary Responsibility: System Owner.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Information Owner or Steward; System Security Officer; System Privacy Officer; Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Information Security Officer; Senior Agency Official for Privacy.

System Development Life Cycle Phase: New – Not Applicable.
Existing – Disposal.

Discussion: When a system is removed from operation, several risk management-related actions are required. Organizations ensure that all controls addressing system disposal are implemented. Examples include media sanitization; configuration management and control; and record retention. Organizational tracking and management systems (including inventory systems) are updated to indicate the system that is being removed from service. Security and privacy posture reports reflect the security and privacy status of the system. Users and application owners hosted on the disposed system are notified as appropriate, and any control inheritance relationships are reviewed and assessed for impact. This task also applies to system components that are removed from operation. Organizations removing a system from operation update the inventory of information systems to reflect the removal.

References: [SP 800-30]; [SP 800-88]; [IR 8062].

APPENDIX A

REFERENCES

LAWS, POLICIES, DIRECTIVES, REGULATIONS, STANDARDS, AND GUIDELINES [102]

LAWS AND EXECUTIVE ORDERS	
[PRIV74]	Privacy Act (P.L. 93-579), December 1974. https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf
[FOIA96]	Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996. https://www.gpo.gov/fdsys/pkg/PLAW-104publ231/html/PLAW-104publ231.htm
[FISMA14]	Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[EO 13800]	Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure
POLICIES, REGULATIONS, DIRECTIVES, AND INSTRUCTIONS	
[OMB A-123]	Office of Management and Budget Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf
[OMB A-130]	Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource*, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
[OMB M-13-13]	Office of Management and Budget Memorandum M-13-13, *Open Data Policy-Managing Information as an Asset*, May 2013. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf
[OMB M-17-25]	Office of Management and Budget Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-25.pdf

[102] The references cited in this appendix are those external publications that directly support the FISMA and Privacy Projects or for which mappings are provided in Appendix E. Additional referential NIST standards, guidelines, and interagency reports are cited throughout this publication, including in the references section of the applicable controls in Chapter Three. Direct links to the NIST website are provided to obtain access to those publications.

[CNSSI 1253] Committee on National Security Systems Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, March 2014.
https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[CNSSI 4009] Committee on National Security Systems Instruction 4009, *Committee on National Security Systems (CNSS) Glossary*, April 2015.
https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[CNSSD 505] Committee on National Security Systems Directive 505, *Supply Chain Risk Management*, August 2017.
https://www.cnss.gov/CNSS/issuances/Directives.cfm

[DODI 5200.44] Department of Defense Instruction 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks* (TSN), July 2017.
http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf

STANDARDS, GUIDELINES, AND REPORTS

[ISO 15026-1] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15026-1:2013, *Systems and software engineering—Systems and software assurance—Part 1: Concepts and vocabulary*, May 2015.
https://www.iso.org/standard/62526.html

[ISO 15288] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15288:2015, *Systems and software engineering—Systems life cycle processes*, May 2015.
https://www.iso.org/standard/63711.html

[ISO 15408-1] International Organization for Standardization/International Electrotechnical Commission 15408-1:2009, *Information technology—Security techniques— Evaluation criteria for IT security—Part 1: Introduction and general model*.
https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

[ISO 15408-2] International Organization for Standardization/International Electrotechnical Commission 15408-2:2008, *Information technology—Security techniques— Evaluation criteria for IT security—Part 2: Security functional requirements*.
https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf

[ISO 15408-3] International Organization for Standardization/International Electrotechnical Commission 15408-3:2008, *Information technology—Security techniques— Evaluation criteria for IT security—Part 3: Security assurance requirements*.
https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

[ISO 29148] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 29148:2011, *Systems and software engineering—Life cycle processes—Requirements engineering*, December 2011.
https://www.iso.org/standard/45171.html

[ISO 27001] International Organization for Standardization/International Electrotechnical Commission 27001:2013, *Information Technology—Security techniques— Information security management systems—Requirements*.
https://www.iso.org/standard/54534.html

[FIPS 199] National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
https://doi.org/10.6028/NIST.FIPS.199

[FIPS 200] National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
https://doi.org/10.6028/NIST.FIPS.200

[SP 800-18] National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
https://doi.org/10.6028/NIST.SP.800-18r1

[SP 800-30] National Institute of Standards and Technology Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, September 2012.
https://doi.org/10.6028/NIST.SP.800-30r1

[SP 800-39] National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.
https://doi.org/10.6028/NIST.SP.800-39

[SP 800-47] National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.
https://doi.org/10.6028/NIST.SP.800-47

[SP 800-53] National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.
https://doi.org/10.6028/NIST.SP.800-53r4

[SP 800-53A] National Institute of Standards and Technology Special Publication 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, July 2008.
https://doi.org/10.6028/NIST.SP.800-53Ar4

[SP 800-55]	National Institute of Standards and Technology Special Publication 800-55, Revision 1, *Performance Measurement Guide for Information Security*, December 2014. https://doi.org/10.6028/NIST.SP.800-55r1
[SP 800-59]	National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003. https://doi.org/10.6028/NIST.SP.800-59
[SP 800-60-1]	National Institute of Standards and Technology Special Publication 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008. https://doi.org/10.6028/NIST.SP.800-60v1r1
[SP 800-60-2]	National Institute of Standards and Technology Special Publication 800-60, Volume 2, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices*, August 2008. https://doi.org/10.6028/NIST.SP.800-60v2r1
[SP 800-64]	National Institute of Standards and Technology Special Publication 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, October 2008. https://doi.org/10.6028/NIST.SP.800-64r2
[SP 800-82]	National Institute of Standards and Technology Special Publication 800-82, Revision 2, *Guide to Industrial Control Systems (ICS) Security*, May 2015. https://doi.org/10.6028/NIST.SP.800-82r2
[SP 800-88]	National Institute of Standards and Technology Special Publication 800-88, *Guidelines for Media Sanitization*, December 2014. https://doi.org/10.6028/NIST.SP.800-88r1
[SP 800-128]	National Institute of Standards and Technology Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011. https://doi.org/10.6028/NIST.SP.800-128
[SP 800-137]	National Institute of Standards and Technology Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011. https://doi.org/10.6028/NIST.SP.800-137
[SP 800-160-1]	National Institute of Standards and Technology Special Publication 800-160, Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, November 2016. https://doi.org/10.6028/NIST.SP.800-160v1
[SP 800-161]	National Institute of Standards and Technology Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, April 2015. https://doi.org/10.6028/NIST.SP.800-161

[SP 800-181] National Institute of Standards and Technology Special Publication 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, August 2017.
https://doi.org/10.6028/NIST.SP.800-181

[IR 8011-1] National Institute of Standards and Technology Interagency Report 8011, Volume 1, *Automation Support for Security Control Assessments: Overview*, June 2017.
https://doi.org/10.6028/NIST.IR.8011-1

[IR 8062] National Institute of Standards and Technology Internal Report 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, January 2017.
https://doi.org/10.6028/NIST.IR.8062

[IR 8179] National Institute of Standards and Technology Internal Report 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components*, April 2018.
https://doi.org/10.6028/NIST.IR.8179

MISCELLANEOUS PUBLICATIONS AND WEBSITES

[DSB 2013] Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, January 2013.
https://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf

[NARA CUI] National Archives and Records Administration, *Controlled Unclassified Information (CUI) Registry*.
https://www.archives.gov/cui

[NIST CSF] National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), Version 1.1, April 2018.
https://www.nist.gov/cyberframework

[OMB FEA] Office of Management and Budget, *Federal Enterprise Architecture (FEA)*.
https://obamawhitehouse.archives.gov/omb/e-gov/fea

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix B provides definitions for terminology used within Special Publication 800-37. Sources for terms used in this publication are cited as applicable. Where no citation is noted, the source of the definition is Special Publication 800-37.

adequate security
[OMB A-130]

Security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

agency
[OMB A-130]

Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency.

allocation

The process an organization employs to determine whether controls are defined as system-specific, hybrid, or common.

The process an organization employs to assign controls to specific information system components responsible for providing a security or privacy capability (e.g., router, server, remote sensor).

application

A software program hosted by an information system.

assessment

See *control assessment*.

assessment plan

The objectives for the control assessments and a detailed roadmap of how to conduct such assessments.

assessor

The individual, group, or organization responsible for conducting a security or privacy assessment.

assignment statement

A control parameter that allows an organization to assign a specific, organization-defined value to the control or control enhancement (e.g., assigning a list of roles to be notified or a value for the frequency of testing).

See *organization-defined control parameters* and *selection statement*.

assurance
[ISO 15026, Adapted]

Grounds for justified confidence that a [security or privacy] claim has been or will be achieved.

Note 1: Assurance is typically obtained relative to a set of specific claims. The scope and focus of such claims may vary (e.g., security claims, safety claims) and the claims themselves may be interrelated.

Note 2: Assurance is obtained through techniques and methods that generate credible evidence to substantiate claims.

audit log
[CNSSI 4009]

A chronological record of system activities, including records of system accesses and operations performed in a given period.

audit trail

A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to result.

authentication
[FIPS 200]

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

authenticity

The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See *authentication*.

authorization boundary
[OMB A-130]

All components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected.

authorization package
[OMB A-130]

The essential information that an authorizing official uses to determine whether to authorize the operation of an information system or the provision of a designated set of common controls. At a minimum, the authorization package includes an executive summary, system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.

authorization to operate
[OMB A-130]

The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.

authorization to use

The official management decision given by an authorizing official to authorize the use of an information system, service, or application based on the information in an existing authorization package generated by another organization, and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of controls in the system, service, or application.

Note: An authorization to use typically applies to cloud and shared systems, services, and applications and is employed when an organization (referred to as the customer organization) chooses to accept the information in an existing authorization package generated by another organization (referred to as the provider organization).

authorizing official
[OMB A-130]

A senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation.

authorizing official designated representative

An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with the authorization process.

availability
[44 U.S.C. Sec. 3542]

Ensuring timely and reliable access to and use of information.

baseline

See *control baseline*.

baseline configuration
[SP 800-128, Adapted]

A documented set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.

capability

A combination of mutually reinforcing controls implemented by technical means, physical means, and procedural means. Such controls are typically selected to achieve a common information security- or privacy-related purpose.

chain of trust
(supply chain)

A certain level of trust in supply chain interactions such that each participant in the consumer-provider relationship provides adequate protection for its component products, systems, and services.

chief information officer
[OMB A-130]

The senior official that provides advice and other assistance to the head of the agency and other senior management personnel of the agency to ensure that IT is acquired and information resources are managed for the agency in a manner that achieves the agency's strategic goals and information resources management goals; and is responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, the information policies and information resources management responsibilities, including the reduction of information collection burdens on the public.

chief information security officer

See *Senior Agency Information Security Officer*.

classified information

See classified national security information.

classified national security information
[CNSSI 4009]

Information that has been determined pursuant to Executive Order (E.O.) 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

commodity service

A system service provided by a commercial service provider to a large and diverse set of consumers. The organization acquiring or receiving the commodity service possesses limited visibility into the management structure and operations of the provider, and while the organization may be able to negotiate service-level agreements, the organization is typically not able to require that the provider implement specific controls.

common control
[OMB A-130]

A security or privacy control that is inherited by multiple information systems or programs.

common control provider

An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., controls inheritable by organizational systems).

common criteria
[CNSSI 4009]

Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems.

compensating controls

The security and privacy controls implemented in lieu of the controls in the baselines described in NIST Special Publication 800-53 that provide equivalent or comparable protection for a system or organization.

component

See *system component*.

confidentiality
[44 U.S.C. Sec. 3542]

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

configuration control
[CNSSI 4009]

Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.

configuration item
[SP 800-128]

An aggregation of system components that is designated for configuration management and treated as a single entity in the configuration management process.

configuration management
[SP 800-128]

A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

configuration settings
[SP 800-128]

The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the system.

continuous monitoring

Maintaining ongoing awareness to support organizational risk decisions.

continuous monitoring program

A program established to collect information in accordance with preestablished metrics, utilizing information readily available in part through implemented security controls.

Note: Privacy and security continuous monitoring strategies and programs can be the same or different strategies and programs.

control assessment

The testing or evaluation of the controls in an information system or an organization to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security or privacy requirements for the system or the organization.

control assessor

The individual, group, or organization responsible for conducting a control assessment. See *assessor*.

control baseline

A collection of controls specifically assembled or brought together to address the protection needs of a group, organization, or community of interest.

control effectiveness

A measure of whether a given control is contributing to the reduction of information security or privacy risk.

control enhancement

Augmentation of a control to build in additional, but related, functionality to the control; increase the strength of the control; or add assurance to the control.

control inheritance
[CNSSI 4009]

A situation in which a system or application receives protection from controls (or portions of controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See *common control*.

control parameter

See *organization-defined control parameter*.

controlled unclassified information
[32 CFR part 2002]

Information that the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

countermeasures
[FIPS 200]

Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of a system. Synonymous with *security controls* and *safeguards*.

cybersecurity
[OMB A-130]

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

developer

A general term that includes developers or manufacturers of systems, system components, or system services; systems integrators; vendors; and product resellers. Development of systems, components, or services can occur internally within organizations or through external entities.

enterprise
[CNSSI 4009]

An organization with a defined mission/goal and a defined boundary, using systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, human resources, financial management, security, and systems, information and mission management. See *organization*.

enterprise architecture
[44 U.S.C. Sec. 3601]

A strategic information asset base, which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture; a target architecture; and a sequencing plan.

environment of operation
[OMB A-130]
The physical surroundings in which an information system processes, stores, and transmits information.

event
[NIST SP 800-61, Adapted]
Any observable occurrence in a system.

executive agency
[OMB A-130]
An executive department specified in 5 U.S.C. Sec. 101; a military department specified in 5 U.S.C. Sec. 102; an independent establishment as defined in 5 U.S.C. Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C. Chapter 91.

external system (or component)
A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required controls or the assessment of control effectiveness.

external system service
A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not a part of, the organizational system) and for which the organization typically has no direct control over the application of required controls or the assessment of control effectiveness.

external system service provider
A provider of external system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.

external network
A network not controlled by the organization.

federal agency
See *executive agency*.

federal enterprise architecture
[OMB FEA]
A business-based framework for governmentwide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.

federal information system
[40 U.S.C. Sec. 11331]
An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

firmware
[CNSSI 4009]
Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs. See *hardware* and *software*.

hardware
[CNSSI 4009]
The material physical components of a system. See *software* and *firmware*.

high-impact system
[FIPS 200]

A system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of high.

hybrid control
[OMB A-130]

A security or privacy control that is implemented for an information system in part as a common control and in part as a system-specific control. See *common control* and *system-specific control*.

impact

With respect to security, the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that individuals could experience when an information system processes their PII.

impact value
[FIPS 199]

The assessed worst-case potential impact that could result from a compromise of the confidentiality, integrity, or availability of information expressed as a value of low, moderate or high.

incident
[44 U.S.C. Sec. 3552]

An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

independent verification and validation
[CNSSI 4009]

A comprehensive review, analysis, and testing, (software and/or hardware) performed by an objective third party to confirm (i.e., verify) that the requirements are correctly defined, and to confirm (i.e., validate) that the system correctly implements the required functionality and security requirements.

industrial control system
[SP 800-82]

General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

information
[OMB A-130]

Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms.

information life cycle
[OMB A-130]

The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion.

information owner

Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

information resources
[44 U.S.C. Sec. 3502]

Information and related resources, such as personnel, equipment, funds, and information technology.

information security
[44 U.S.C. Sec. 3542]

The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

information security architecture
[OMB A-130]

An embedded, integral part of the enterprise architecture that describes the structure and behavior of the enterprise security processes, security systems, personnel and organizational subunits, showing their alignment with the enterprise's mission and strategic plans. See *security architecture*.

information security program plan
[OMB A-130]

Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.

information security risk
[SP 800-30]

The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or systems.

information steward

An agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

information system
[44 U.S.C. Sec. 3502]

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

information system boundary

See *authorization boundary*.

information system security officer
[CNSSI 4009]

Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.

Information system security plan
[OMB A-130]

A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. See *system security plan*.

information technology
[OMB A-130]

Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. Information technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use.

information technology product

See *system component*.

information type
[FIPS 199]

A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management) defined by an organization or in some instances, by a specific law, executive order, directive, policy, or regulation.

interface
[CNSSI 4009]

Common boundary between independent systems or modules where interactions take place.

integrity
[44 U.S.C. Sec. 3542]

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

joint authorization

Authorization involving multiple authorizing officials.

low-impact system
[FIPS 200]

A system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS Publication 199 potential impact value of low.

media
[FIPS 200]

Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration memory chips, and printouts (but excluding display media) onto which information is recorded, stored, or printed within a system.

moderate-impact system
[FIPS 200]

A system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of moderate and no security objective is assigned a potential impact value of high.

national security system
[44 U.S.C. Sec. 3542]

Any system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

network

A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

network access

Access to a system by a user (or a process acting on behalf of a user) communicating through a network including, for example, a local area network, a wide area network, and Internet.

operational technology

Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

operations technology

See *operational technology*.

organization
[FIPS 200, Adapted]

An entity of any size, complexity, or positioning within an organizational structure including, for example, federal agencies, private enterprises, academic institutions, state, local, or tribal governments, or as appropriate, any of their operational elements.

organization-defined control parameter

The variable part of a control or control enhancement that can be instantiated by an organization during the tailoring process by either assigning an organization-defined value or selecting a value from a pre-defined list provided as part of the control or control enhancement.

overlay
[OMB A-130]

A specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. See *tailoring* and *tailored control baseline*.

personally identifiable information
[OMB A-130]

Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

plan of action and milestones

A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

potential impact
[FIPS 199]

The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (FIPS Publication 199 low); a serious adverse effect (FIPS Publication 199 moderate); or a severe or catastrophic adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.

privacy architect

Individual, group, or organization responsible for ensuring that the system privacy requirements necessary to protect individuals' privacy are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and information systems processing PII.

privacy architecture

An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's privacy protection processes, technical measures, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.

privacy control
[OMB A-130]

The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.

Note: Controls can be selected to achieve multiple objectives; those controls that are selected to achieve both security and privacy objectives require a degree of collaboration between the organization's information security program and privacy program.

privacy control assessment
[OMB A-130]

The assessment of privacy controls to determine whether the controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks. A privacy control assessment is both an assessment and a formal document detailing the process and the outcome of the assessment.

privacy control baseline

A collection of controls specifically assembled or brought together by a group, organization, or community of interest to address the privacy protection needs of individuals.

privacy impact assessment
[OMB A-130]

An analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis.

privacy plan
[OMB A-130]

A formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls.

privacy posture

The privacy posture represents the status of the information systems and information resources (e.g., personnel, equipment, funds, and information technology) within an organization based on information assurance resources (e.g., people, hardware, software, policies, procedures) and the capabilities in place to comply with applicable privacy requirements and manage privacy risks and to react as the situation changes.

privacy program plan
[OMB A-130]

A formal document that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.

privacy requirement

A requirement that applies to an information system or an organization that is derived from applicable laws, executive orders, directives, policies, standards, regulations, procedures, and/or mission/business needs with respect to privacy.

Note: The term *privacy requirement* can be used in a variety of contexts from high-level policy-related activities to low-level implementation-related activities in system development and engineering disciplines.

privacy-related information

Information that describes the privacy posture of an information system or organization.

provenance

The chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data.

reciprocity

Agreement among participating organizations to accept each other's security assessments to reuse system resources and/or to accept each other's assessed security posture to share information.

records
[44 U.S.C. § 3301]

All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

resilience
[CNSSI 4009]

The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

risk
[OMB A-130]

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

risk assessment
[SP 800-30]

The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system.

risk executive (function)

An individual or group within an organization that helps to ensure that security risk-related considerations for individual systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and managing risk from individual systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.

risk management
[OMB A-130]

The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.

risk mitigation
[CNSSI 4009]

Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

risk response
[OMB A-130]

Accepting, avoiding, mitigating, sharing, or transferring risk to agency operations, agency assets, individuals, other organizations, or the Nation.

sanitization
[SP 800-88]

A process to render access to target data on the media infeasible for a given level of effort. Clear, purge, and destroy are actions that can be taken to sanitize media.

scoping considerations

A part of tailoring guidance providing organizations with specific considerations on the applicability and implementation of controls in the control baselines. Considerations include policy/regulatory, technology, physical infrastructure, system component allocation, operational/environmental, public access, scalability, common control, and security objective.

security
[CNSSI 4009]

A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization’s risk management approach.

security architect

Individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization’s core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes.

security architecture
[SP 800-39]

An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans. See *information security architecture*.

[SP 800-160-1]

A set of physical and logical security-relevant representations (i.e., views) of system architecture that conveys information about how the system is partitioned into security domains and makes use of security-relevant elements to enforce security policies within and between security domains based on how data and information must be protected.

Note: The security architecture reflects security domains, the placement of security-relevant elements within the security domains, the interconnections and trust relationships between the security-relevant elements, and the behavior and interactions between the security-relevant elements. The security architecture, similar to the system architecture, may be expressed at different levels of abstraction and with different scopes.

security categorization

The process of determining the security category for information or a system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS Publication 199 for other than national security systems. See *security category*.

security category
[OMB A-130]

The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on agency operations, agency assets, individuals, other organizations, and the Nation.

security control
[OMB A-130]

The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.

security control assessment
[OMB A-130]

The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

security control baseline
[OMB A-130]

The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system. See also *control baseline*.

security objective
[FIPS 199]

Confidentiality, integrity, or availability.

security plan

See *system security plan*.

security posture
[CNSSI 4009]

The security status of an enterprise's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes. Synonymous with *security status*.

security requirement
[FIPS 200, Adapted]

A requirement levied on an information system or an organization that is derived from applicable laws, executive orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted.

Note: Security requirements can be used in a variety of contexts from high-level policy-related activities to low-level implementation-related activities in system development and engineering disciplines.

security-related information

Information within the system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data.

selection statement

A control parameter that allows an organization to select a value from a list of pre-defined values provided as part of the control or control enhancement (e.g., selecting to either restrict an action or prohibit an action).

See *assignment statement* and *organization-defined control parameter*.

senior agency information security officer
[44 U.S.C. Sec. 3544]

Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.

senior agency official for privacy
[OMB A-130]

The senior official, designated by the head of each agency, who has agency-wide responsibility for privacy, including implementation of privacy protections; compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals.

software
[CNSSI 4009]

Computer programs and associated data that may be dynamically written or modified during execution.

subsystem

A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.

supply chain
[OMB A-130]

Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.

supply chain risk
[OMB A-130]

Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

supply chain risk management
[OMB A-130]

The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of information and communications technology product and service supply chains.

system
[CNSSI 4009]

Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. See *information system*.

Note: Systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

[ISO 15288]

Combination of interacting elements organized to achieve one or more stated purposes.

Note 1: There are many types of systems. Examples include: general and special-purpose information systems; command, control, and communication systems; crypto modules; central processing unit and graphics processor boards; industrial/process control systems; flight control systems; weapons, targeting, and fire control systems; medical devices and treatment systems; financial, banking, and merchandising transaction systems; and social networking systems.

Note 2: The interacting elements in the definition of system include hardware, software, data, humans, processes, facilities, materials, and naturally occurring physical entities.

Note 3: System of systems is included in the definition of system.

system boundary

See *authorization boundary*.

system component
[SP 800-128]

A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware.

system element
[ISO 15288]

Member of a set of elements that constitute a system.

Note 1: A system element can be a discrete component, product, service, subsystem, system, infrastructure, or enterprise.

Note 2: Each element of the system is implemented to fulfill specified requirements.

Note 3: The recursive nature of the term allows the term *system* to apply equally when referring to a discrete component or to a large, complex, geographically distributed system-of-systems.

Note 4: System elements are implemented by: hardware, software, and firmware that perform operations on data/information; physical structures, devices, and components in the environment of operation; and the people, processes, and procedures for operating, sustaining, and supporting the system elements.

Note 5: System elements and *information resources* (as defined at 44 U.S.C. Sec. 3502 and in this document) are interchangeable terms as used in this document.

system development life cycle

The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

system privacy officer

Individual with assigned responsibility for maintaining the appropriate operational privacy posture for a system or program.

systems privacy engineer

Individual assigned responsibility for conducting systems privacy engineering activities.

systems privacy engineering

Process that captures and refines privacy requirements and ensures their integration into information technology component products and information systems through purposeful privacy design or configuration.

systems security engineer

Individual assigned responsibility for conducting systems security engineering activities.

systems security engineering

Process that captures and refines security requirements and ensures their integration into information technology component products and information systems through purposeful security design or configuration.

system security officer

Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.

system security plan

A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. See *information system security plan*.

Note: The security plan describes the authorization boundary; the environment in which the system operates; the relationships with or connections to other systems; and how the security requirements are implemented.

system-related privacy risk
[OMB A-130]

Risk to an individual or individuals associated with the agency's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of their PII. See *risk*.

system-related security risk
[SP 800-30]

Risk that arises through the loss of confidentiality, integrity, or availability of information or systems and that considers impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation. See *risk*.

system-specific control
[OMB A-130]

A security or privacy control for an information system that is implemented at the system level and is not inherited by any other information system.

tailored control baseline

A set of controls resulting from the application of tailoring guidance to a control baseline. See *tailoring* and *overlay*.

tailoring
[OMB A-130]

The process by which security control baselines are modified by identifying and designating common controls; applying scoping considerations; selecting compensating controls; assigning specific values to agency-defined control parameters; supplementing baselines with additional controls or control enhancements; and providing additional specification information for control implementation. The tailoring process may also be applied to privacy controls. See *overlay*.

threat
[CNSSI 4009, Adapted]

Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

threat source
[FIPS 200]

The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. See *threat agent*.

trustworthiness
[CNSSI 4009]

The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.

trustworthiness
(system)

The degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats and individuals' privacy.

trustworthy information system
[OMB A-130]

An information system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.

system user

Individual, or (system) process acting on behalf of an individual, authorized to access a system.

vulnerability
[CNSSI 4009]

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Note: The term *weakness* is synonymous for *deficiency*. Weakness may result in security and/or privacy risks.

vulnerability assessment
[CNSSI 4009]

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CUI	Controlled Unclassified Information
DoD	Department of Defense
EO	Executive Order
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FOCI	Foreign Ownership, Control, or Influence
GRC	Governance Risk Compliance
GSA	General Services Administration
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISCM	Information Security Continuous Monitoring
IT	Information Technology
IR	Internal Report or Interagency Report
ISO	International Organization for Standardization
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OT	Operations Technology
PCM	Privacy Continuous Monitoring
PII	Personally Identifiable Information
PL	Public Law
RMF	Risk Management Framework

SAOP	Senior Agency Official for Privacy
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SecCM	Security-focused Configuration Management
SP	Special Publication

APPENDIX D

ROLES AND RESPONSIBILITIES

KEY PARTICIPANTS IN THE RISK MANAGEMENT PROCESS

The following sections describe the roles and responsibilities of key participants involved in an organization's risk management process.[103] Recognizing that organizations have varying missions, business functions, and organizational structures, there may be differences in naming conventions for risk management roles and how risk management responsibilities are allocated among organizational personnel. This includes, for example, multiple individuals filling a single role or one individual filling multiple roles.[104] However, the basic functions remain the same. The application of the RMF described in this publication is flexible, allowing organizations to effectively accomplish the intent of the specific tasks within their respective organizational structures to best manage security and privacy risks. Many risk management roles defined in this publication have counterpart roles in the SDLC processes carried out by organizations. Organizations align their risk management roles with similar (or complementary) roles defined for the SDLC whenever possible.[105]

AUTHORIZING OFFICIAL

The *authorizing official* is a senior official or executive with the authority to formally assume responsibility and accountability for operating a system; providing common controls inherited by organizational systems; or using a system, service, or application from an external provider. The authorizing official is the only organizational official who can accept the security and privacy risk to organizational operations, organizational assets, and individuals.[106] Authorizing officials typically have budgetary oversight for the system or are responsible for the mission and/or business operations supported by the system. Accordingly, authorizing officials are in management positions with a level of authority commensurate with understanding and accepting such security and privacy risks. Authorizing officials approve plans, memorandums of agreement or understanding, plans of action and milestones, and determine whether significant changes in the information systems or environments of operation require reauthorization.

Authorizing officials coordinate their activities with common control providers, system owners, chief information officers, senior agency information security officers, senior agency officials for privacy, system security and privacy officers, control assessors, senior accountable officials for risk management/risk executive (function), and other interested parties during the authorization process. With the increasing complexity of the mission/business processes in an organization, partnership arrangements, and the use of shared services, it is possible that a system may

[103] Organizations may define other roles to support the risk management process.

[104] Organizations ensure that there are no conflicts of interest when assigning the same individual to multiple risk management roles. See RMF *Prepare-Organization Level* step, Task P-1.

[105] For example, the SDLC role of system developer or program manager can be aligned with the role of system owner; and the role of mission or business owner can be aligned with the role of authorizing official. [SP 800-64] provides guidance on information security in the SDLC.

[106] The responsibility and accountability of authorizing officials described in [FIPS 200] was extended in [SP 800-53] to include risks to other organizations and the Nation.

involve co-authorizing officials.[107] If so, agreements are established between the co-authorizing officials and documented in the security and privacy plans. Authorizing officials are responsible and accountable for ensuring that authorization activities and functions that are delegated to authorizing official designated representatives are carried out as specified. For federal agencies, the role of authorizing official is an inherent U.S. Government function and is assigned to government personnel only.

AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE

The *authorizing official designated representative* is an organizational official designated by the authorizing official who is empowered to act on behalf of the authorizing official to coordinate and conduct the day-to-day activities associated with managing risk to information systems and organizations. This includes carrying out many of the activities related to the execution of the RMF. The only activity that cannot be delegated by the authorizing official to the designated representative is the authorization decision and signing of the associated authorization decision document (i.e., the acceptance of risk).

CHIEF ACQUISITION OFFICER

The *chief acquisition officer* is an organizational official designated by the head of an agency to advise and assist the agency head and other agency officials to ensure that the mission of the agency is achieved through the management of the agency's acquisition activities. The chief acquisition officer monitors the performance of acquisition activities and programs; establishes clear lines of authority, accountability, and responsibility for acquisition decision making within the agency; manages the direction and implementation of acquisition policy for the agency; and establishes policies, procedures, and practices that promote full and open competition from responsible sources to fulfil best value requirements considering the nature of the property or service procured. The Chief Acquisition Officer coordinates with mission or business owners, authorizing officials, system owners, common control providers, senior agency information security officer, senior agency official for privacy, risk executive (function), and senior agency official for risk management to ensure that security and privacy requirements are clearly defined in organizational procurements and acquisitions.

CHIEF INFORMATION OFFICER

The *chief information officer*[108] is an organizational official responsible for designating a senior agency information security officer; developing and maintaining security policies, procedures, and control techniques to address security requirements; overseeing personnel with significant responsibilities for security and ensuring that the personnel are adequately trained; assisting senior organizational officials concerning their security responsibilities; and reporting to the head of the agency on the effectiveness of the organization's security program, including progress of remedial actions. The chief information officer, with the support of the senior agency official for risk management, the risk executive (function), and the senior agency information security officer, works closely with authorizing officials and their designated representatives to help ensure that:

[107] [OMB A-130] provides additional information about authorizing officials and co-authorizing officials.

[108] When an organization has not designated a formal chief information officer position, [FISMA14] requires that the associated responsibilities be handled by a comparable organizational official.

- An organization-wide security program is effectively implemented resulting in adequate security for all organizational systems and environments of operation;
- Security and supply chain risk management considerations are integrated into programming/planning/budgeting cycles, enterprise architectures, the SDLC, and acquisitions;
- Organizational systems and common controls are covered by approved security plans and possess current authorizations;
- Security-related activities required across the organization are accomplished in an efficient, cost-effective, and timely manner; and
- There is centralized reporting of security-related activities.

The chief information officer and authorizing officials determine the allocation of resources dedicated to the protection of systems supporting the organization's missions and business functions based on organizational priorities. For information systems that process personally identifiable information, the chief information officer and authorizing officials coordinate any determination about the allocation of resources dedicated to the protection of those systems with the senior agency official for privacy. For selected systems, the chief information officer may be designated as an authorizing official or a co-authorizing official with other senior organizational officials. The role of chief information officer is an inherent U.S. Government function and is assigned to government personnel only.

COMMON CONTROL PROVIDER

The *common control provider* is an individual, group, or organization that is responsible for the implementation, assessment, and monitoring of common controls (i.e., controls inherited by organizational systems).[109] Common control providers also are responsible for ensuring the documentation of organization-defined common controls in security and privacy plans (or equivalent documents prescribed by the organization); ensuring that required assessments of the common controls are conducted by qualified assessors with an appropriate level of independence; documenting assessment findings in control assessment reports; and producing plans of action and milestones for controls having deficiencies. Security and privacy plans, security and privacy assessment reports, and plans of action and milestones for common controls (or summary of such information) are made available to the system owners of systems inheriting common controls after the information is reviewed and approved by the authorizing officials accountable for those common controls.

The senior agency official for privacy is responsible for designating which privacy controls may be treated as common controls. Privacy controls that are designated as common controls are documented in the organization’s privacy program plan.[110] The senior agency official for privacy

[109] Organizations can have multiple common control providers depending on how security and privacy responsibilities are allocated organization-wide. Common control providers may be *system owners* when the common controls are resident within an organizational system.

[110] A privacy program plan is a formal document that provides an overview of an agency’s privacy program, including a description of the structure of the privacy program; the role of the senior agency official for privacy and other privacy officials and staff; the strategic goals and objectives of the privacy program; the resources dedicated to the privacy program; and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.

has oversight responsibility for common controls in place or planned for meeting applicable privacy requirements and managing privacy risks and is responsible for assessing those controls. At the discretion of the organization, privacy controls that are designated as common controls may be assessed by an independent assessor. In all cases, however, the senior agency official for privacy retains responsibility and accountability for the organization's privacy program, including any privacy functions performed by independent assessors. Privacy plans and privacy control assessment reports are made available to systems owners whose systems inherit privacy controls that are designated as common controls.

CONTROL ASSESSOR

The *control assessor* is an individual, group, or organization responsible for conducting a comprehensive assessment of the controls and control enhancements implemented within or inherited by a system to determine the effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization). The system owner and common control provider rely on the security and privacy expertise and judgment of the assessor to assess the controls implemented within and inherited by the information system using the assessment procedures specified in the security and privacy assessment plans. Multiple control assessors who are differentiated by their expertise in specific control requirements or technologies may be required to conduct the assessment effectively. Prior to initiating the control assessment, assessors review the security and privacy plans to facilitate development of the assessment plans. Control assessors provide an assessment of the severity of the deficiencies discovered in the system and its environment of operation and can recommend corrective actions to address the identified vulnerabilities. Finally, control assessors prepare security and privacy assessment reports containing the results and findings from the assessment.

The required level of assessor independence is determined by the authorizing official based on laws, executive orders, directives, regulations, policies, standards, or guidelines. When a control assessment is conducted in support of an authorization decision or ongoing authorization, the authorizing official makes an explicit determination of the degree of independence required. Assessor independence is a factor in preserving an impartial and unbiased assessment process; determining the credibility of the assessment results; and ensuring that the authorizing official receives objective information to make an informed, risk-based authorization decision.

The senior agency official for privacy is responsible for assessing privacy controls and for providing privacy-related information to the authorizing official. At the discretion of the organization, privacy controls may be assessed by an independent assessor. However, in all cases, the senior agency official for privacy retains responsibility and accountability for the privacy program of the organization, including any privacy functions performed by the independent assessors.

ENTERPRISE ARCHITECT

The *enterprise architect* is an individual or group responsible for working with the leadership and subject matter experts in an organization to build a holistic view of the organization's missions and business functions, mission/business processes, information, and information technology assets. With respect to information security and privacy, enterprise architects:

- Implement an enterprise architecture strategy that facilitates effective security and privacy solutions;
- Coordinate with security and privacy architects to determine the optimal placement of systems/system elements within the enterprise architecture and to address security and privacy issues between systems and the enterprise architecture;
- Assist in reducing complexity within the IT infrastructure to facilitate security;
- Assist with determining appropriate control implementations and initial configuration baselines as they relate to the enterprise architecture;
- Collaborate with system owners and authorizing officials to facilitate authorization boundary determinations and allocation of controls to system elements;
- Serve as part of the Risk Executive (function); and
- Assist with integration of the organizational risk management strategy and system-level security and privacy requirements into program, planning, and budgeting activities, the SDLC, acquisition processes, and systems engineering processes.

HEAD OF AGENCY

The *head of agency* is responsible and accountable for providing information security protections commensurate with the risk to organizational operations and assets, individuals, other organizations, and the Nation—that is, risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; and the information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. The head of agency is also the senior official in an organization with the responsibility for ensuring that privacy interests are protected and that PII is managed responsibly within the organization. The heads of agencies ensure that:

- Information security and privacy management processes are integrated with strategic and operational planning processes;
- Senior officials within the organization provide information security for the information and systems that support the operations and assets under their control;
- Senior agency officials for privacy are designated who are responsible and accountable for ensuring compliance with applicable privacy requirements, managing privacy risk, and the organization’s privacy program; and
- The organization has adequately trained personnel to assist in complying with security and privacy requirements in legislation, executive orders, policies, directives, instructions, standards, and guidelines.

The head of agency establishes the organizational commitment and the actions required to effectively manage security and privacy risk and protect the missions and business functions being carried out by the organization. The head of agency or establishes security and privacy accountability and provides active support and oversight of monitoring and improvement for the security and privacy programs. Senior leadership commitment to security and privacy establishes a level of due diligence within the organization that promotes a climate for mission and business success.

INFORMATION OWNER OR STEWARD

The *information owner or steward* is an organizational official with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal. In information-sharing environments, the information owner/steward is responsible for establishing the rules for appropriate use and protection of the information and retains that responsibility even when the information is shared with or provided to other organizations. The owner/steward of the information processed, stored, or transmitted by a system may or may not be the same individual as the system owner. An individual system may contain information from multiple information owners/stewards. Information owners/stewards provide input to system owners regarding the security and privacy requirements and controls for the systems where the information is processed, stored, or transmitted.

MSSION OR BUSINESS OWNER

The *mission or business owner* is the senior official or executive within an organization with specific mission or line of business responsibilities and that has a security or privacy interest in the organizational systems supporting those missions or lines of business. Mission or business owners are key stakeholders that have a significant role in establishing organizational mission and business processes and the protection needs and security and privacy requirements that ensure the successful conduct of the organization's missions and business operations. Mission and business owners provide essential inputs to the risk management strategy, play an active part in the SDLC, and may also serve in the role of authorizing official.

RISK EXECUTIVE (FUNCTION)

The *risk executive (function)* is an individual or group within an organization that provides a comprehensive, organization-wide approach to risk management. The risk executive (function) serves as the common risk management resource for senior leaders, executives, and managers, mission/business owners, chief information officers, senior agency information security officers, senior agency officials for privacy, system owners, common control providers, enterprise architects, security architects, systems security or privacy engineers, system security or privacy officers, and any other stakeholders having a vested interest in the mission/business success of organizations. The risk executive (function) is an inherent U.S. Government function and is assigned to government personnel only.

The risk executive (function) ensures that risk-related considerations for systems (including authorization decisions for those systems and the common controls inherited by those systems), are viewed from an organization-wide perspective regarding the organization's strategic goals and objectives in carrying out its core missions and business functions. The risk executive (function) ensures that managing risk is consistent throughout the organization, reflects organizational risk tolerance, and is considered along with other types of risk to ensure mission/business success. The risk executive (function) coordinates with senior leaders and executives to:

- Establish risk management roles and responsibilities;

- Develop and implement an organization-wide *risk management strategy* that provides a strategic view of security-related risks for the organization[111] and that guides and informs organizational risk decisions (including how risk is framed, assessed, responded to, and monitored over time);
- Provide a comprehensive, organization-wide, holistic approach for addressing risk—an approach that provides a greater understanding of the integrated operations of the organization;
- Manage threat, vulnerability, and security, privacy, and supply chain risk information for organizational systems and the environments in which the systems operate;
- Establish organization-wide forums to consider all types and sources of risk (including aggregated risk);
- Identify the organizational risk posture based on the aggregated risk from the operation and use of systems and the respective environments of operation for which the organization is responsible;
- Provide oversight for the risk management activities carried out by organizations to help ensure consistent and effective risk-based decisions;
- Develop a broad-based understanding of risk regarding the strategic view of organizations and their integrated operations;
- Establish effective vehicles and serve as a focal point for communicating and sharing risk-related information among key stakeholders (e.g., authorization officials and other senior leaders) internally and externally to organizations;
- Specify the degree of autonomy for subordinate organizations permitted by parent organizations regarding framing, assessing, responding to, and monitoring risk;
- Promote cooperation and collaboration among authorizing officials to include authorization actions requiring shared responsibility (e.g., joint authorizations);
- Provide an organization-wide forum to consider all sources of risk (including aggregated risk) to organizational operations and assets, individuals, other organizations, and the Nation;
- Ensure that authorization decisions consider all factors necessary for mission and business success; and
- Ensure shared responsibility for supporting organizational missions and business functions using external providers receives the needed visibility and is elevated to appropriate decision-making authorities.

The risk executive (function) presumes neither a specific organizational structure nor formal responsibility assigned to any one individual or group within the organization. Heads of agencies or organizations may choose to retain the risk executive (function) or to delegate the function. The risk executive (function) requires a mix of skills, expertise, and perspectives to understand the strategic goals and objectives of organizations, organizational missions/business functions, technical possibilities and constraints, and key mandates and guidance that shape organizational

[111] Authorizing officials may have narrow or localized perspectives in rendering authorization decisions without fully understanding or explicitly accepting the organization-wide risks being incurred from such decisions.

operations. To provide this needed mixture, the risk executive (function) can be filled by a single individual or office (supported by an expert staff) or by a designated group (e.g., a risk board, executive steering committee, executive leadership council). The risk executive (function) fits into the organizational governance structure in such a way as to facilitate efficiency and effectiveness.

SECURITY OR PRIVACY ARCHITECT

The *security or privacy architect* is an individual, group, or organization responsible for ensuring that stakeholder protection needs and the corresponding system requirements necessary to protect organizational missions and business functions and individuals' privacy are adequately addressed in the enterprise architecture including reference models, segment architectures, and solution architectures (systems supporting mission and business processes). The security or privacy architect serves as the primary liaison between the enterprise architect and the systems security or privacy engineer and coordinates with system owners, common control providers, and system security or privacy officers on the allocation of controls. Security or privacy architects, in coordination with system security or privacy officers, advise authorizing officials, chief information officers, senior accountable officials for risk management or risk executive (function), senior agency information security officers, and senior agency officials for privacy on a range of security and privacy issues. Examples include establishing authorization boundaries; establishing security or privacy alerts; assessing the severity of deficiencies in the system or controls; developing plans of action and milestones; creating risk mitigation approaches; and potential adverse effects of identified vulnerabilities or privacy risks.

When the security architect and privacy architect are separate roles, the security architect is generally responsible for aspects of the enterprise architecture that protect information and information systems from unauthorized system activity or behavior to provide confidentiality, integrity, and availability. The privacy architect is responsible for aspects of the enterprise architecture that ensure compliance with privacy requirements and manage the privacy risks to individuals associated with the processing of PII. Security and privacy architect responsibilities overlap regarding aspects of the enterprise architecture that protect the security of PII.

SENIOR ACCOUNTABLE OFFICIAL FOR RISK MANAGEMENT

The *senior accountable official for risk management* is the individual that leads and manages the risk executive (function) in an organization and is responsible for aligning information security and privacy risk management processes with strategic, operational, and budgetary planning processes. This official is the agency head or an individual designated by the agency head. The senior accountable official for risk management determines the organizational structure and responsibilities of the risk executive (function). The head of the agency, in coordination with the senior accountable official for risk management, may retain the risk executive (function) or delegate the function to another organizational official or group. The senior accountable official for risk management and the risk executive (function) are inherent U.S. Government functions and are assigned to government personnel only.

SENIOR AGENCY INFORMATION SECURITY OFFICER

The *senior agency information security officer* is an organizational official responsible for carrying out the chief information officer security responsibilities under FISMA, and serving as the primary liaison for the chief information officer to the organization's authorizing officials, system owners, common control providers, and system security officers. The senior agency information security officer is also responsible for coordinating with the senior agency official for privacy to ensure coordination between privacy and information security programs. The senior agency information security officer possesses the professional qualifications, including training and experience, required to administer security program functions; maintains security duties as a primary responsibility; and heads an office with the specific mission and resources to assist the organization in achieving trustworthy, secure information and systems in accordance with the requirements in FISMA. The senior agency information security officer may serve as authorizing official designated representative or as a security control assessor. The role of senior agency information security officer is an inherent U.S. Government function and is therefore assigned to government personnel only. Organizations may also refer to the senior agency information security officer as the senior information security officer or chief information security officer.

SENIOR AGENCY OFFICIAL FOR PRIVACY

The *senior agency official for privacy* is the senior official or executive with agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risk. Among other things, the senior agency official for privacy is responsible for:

- Coordinating with the senior agency information security officer to ensure coordination of privacy and information security activities;
- Reviewing and approving the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information;
- Designating which privacy controls will be treated as program management, common, system-specific, and hybrid privacy controls;
- Identifying assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks;
- Reviewing and approving privacy plans for information systems prior to authorization, reauthorization, or ongoing authorization;
- Reviewing authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information to ensure compliance with privacy requirements and manage privacy risks;
- Conducting and documenting the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency; and
- Establishing and maintaining a privacy continuous monitoring program to maintain ongoing awareness of privacy risks and assess privacy controls at a frequency sufficient to ensure compliance with privacy requirements and manage privacy risks.

The role of senior agency official for privacy is an inherent U.S. Government function and is therefore assigned to government personnel only.

SYSTEM ADMINISTRATOR

The *system administrator* is an individual, group, or organization responsible for setting up and maintaining a system or specific components of a system. System administrator responsibilities include, for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup, recovery, and reconstitution activities; implementing controls; and adhering to and enforcing organizational security and privacy policies and procedures. The system administrator role includes other types of system administrators including, for example, database administrators, network administrators, application administrators, and web administrators.

SYSTEM OWNER

The *system owner* is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system.[112] The system owner is responsible for addressing the operational interests of the user community (i.e., users who require access to the system to satisfy mission, business, or operational requirements) and for ensuring compliance with security requirements. In coordination with the system security and privacy officers, the system owner is responsible for the development and maintenance of the security and privacy plans and ensures that the system is operated in accordance with the selected and implemented controls.

In coordination with the information owner/steward, the system owner decides who has access to the system (and with what types of privileges or access rights).[113] The system owner ensures that system users and support personnel receive the requisite security and privacy training. Based on guidance from the authorizing official, the system owner informs organizational officials of the need to conduct the authorization, ensures that resources are available for the effort, and provides the required system access, information, and documentation to control assessors. The system owner receives the security and privacy assessment results from the control assessors. After taking appropriate steps to reduce or eliminate vulnerabilities or security and privacy risks, the system owner assembles the authorization package and submits the package to the authorizing official or the authorizing official designated representative for adjudication.[114]

SYSTEM SECURITY OR PRIVACY OFFICER

The *system security or privacy officer*[115] is an individual responsible for ensuring that the security and privacy posture is maintained for an organizational system and works in close collaboration

[112] Organizations may refer to system owners as program managers or business/asset owners.

[113] The responsibility for deciding who has access to specific information within an organizational system (and with what types of privileges or access rights) may reside with the information owner/steward.

[114] The authorizing official may choose to designate an individual other than the system owner to compile and assemble the information for the authorization package. In this situation, the designated individual coordinates the compilation and assembly activities with the system owner.

[115] Organizations may define a *system security manager* or *security manager* role with similar responsibilities as a system security officer or with oversight responsibilities for a security program. In these situations, system security officers may, at the discretion of the organization, report directly to system security managers or security managers. Organizations may assign equivalent responsibilities for privacy to separate individuals with appropriate subject matter expertise.

with the system owner. The system security or privacy officer also serves as a principal advisor on all matters, technical and otherwise, involving the controls for the system. The system security or privacy officer has the knowledge and expertise to manage the security or privacy aspects of an organizational system and, in many organizations, is assigned responsibility for the day-to-day system security or privacy operations. This responsibility may also include, but is not limited to, physical and environmental protection; personnel security; incident handling; and security and privacy training and awareness. The system security or privacy officer may be called on to assist in the development of the system-level security and privacy policies and procedures and to ensure compliance with those policies and procedures. In close coordination with the system owner, the system security or privacy officer often plays an active role in the monitoring of a system and its environment of operation to include developing and updating security and privacy plans, managing and controlling changes to the system, and assessing the security or privacy impact of those changes.

When the system security officer and system privacy officer are separate roles, the system security officer is generally responsible for aspects of the system that protect information and information systems from unauthorized system activity or behavior to provide confidentiality, integrity, and availability. The system privacy officer is responsible for aspects of the system that ensure compliance with privacy requirements and manage the privacy risks to individuals associated with the processing of PII. The responsibilities of system security officers and system privacy officers overlap regarding aspects of the system that protect the security of PII.

SYSTEM USER

The *system user* is an individual or (system) process acting on behalf of an individual, that is authorized to access information and information systems to perform assigned duties. System user responsibilities include, but are not limited to, adhering to organizational policies that govern acceptable use of organizational systems; using the organization-provided information technology resources for defined purposes only; and reporting anomalous or suspicious system behavior.

SYSTEMS SECURITY OR PRIVACY ENGINEER

The *systems security or privacy engineer* is an individual, group, or organization responsible for conducting systems security or privacy engineering activities as part of the SDLC. Systems security and privacy engineering is a process that captures and refines security and privacy requirements for systems and ensures that the requirements are effectively integrated into systems and system components through security or privacy architecting, design, development, and configuration. Systems security or privacy engineers are part of the development team—designing and developing organizational systems or upgrading existing systems along with ensuring continuous monitoring requirements are addressed at the system level. Systems security or privacy engineers employ best practices when implementing controls including software engineering methodologies; system and security or privacy engineering principles; secure or privacy-enhancing design, secure or privacy-enhancing architecture, and secure or privacy-enhancing coding techniques. Systems security or privacy engineers coordinate security and privacy activities with senior agency information security officers, senior agency officials for privacy, security and privacy architects, system owners, common control providers, and system security or privacy officers.

When the systems security engineer and privacy engineer are separate roles, the systems security engineer is generally responsible for those activities associated with protecting information and information systems from unauthorized system activity or behavior to provide confidentiality, integrity, and availability. The privacy engineer is responsible for those activities associated with ensuring compliance with privacy requirements and managing the privacy risks to individuals associated with the processing of PII. The responsibilities of systems security engineers and privacy engineers overlap regarding activities associated with protecting the security of PII.

APPENDIX E

SUMMARY OF RMF TASKS

RMF TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

TABLE E-1: PREPARE TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
Organization Level		
TASK P-1 **Risk Management Roles** Identify and assign individuals to specific roles associated with security and privacy risk management.	• Head of Agency • Chief Information Officer • Senior Agency Official for Privacy	• Authorizing Official or Authorizing Official Designated Representative • Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer
TASK P-2 **Risk Management Strategy** Establish a risk management strategy for the organization that includes a determination of risk tolerance.	• Head of Agency	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK P-3 **Risk Assessment—Organization** Assess organization-wide security and privacy risk and update the results on an ongoing basis.	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy	• Chief Information Officer • Authorizing Official or Authorizing Official Designated Representative • Mission or Business Owner
TASK P-4 **Organization-Wide Tailored Control Baselines and Profiles (Optional)** Establish, document, and publish organization-wide tailored control baselines and/or profiles.	• Mission or Business Owner • Senior Accountable Official for Risk Management or Risk Executive (Function)	• Chief Information Officer • Authorizing Official or Authorizing Official Designated Representative • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK P-5 **Common Control Identification** Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems.	• Senior Agency Information Security Officer • Senior Agency Official for Privacy	• Mission or Business Owner • Senior Accountable Official for Risk Management or Risk Executive (Function) • Chief Information Officer • Authorizing Official or Authorizing Official Designated Representative • Common Control Provider • System Owner

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK P-6 **Impact-Level Prioritization (Optional)** Prioritize organizational systems with the same impact level.	• Senior Accountable Official for Risk Management or Risk Executive (Function)	• Senior Agency Information Security Officer • Senior Agency Official for Privacy • Mission or Business Owner • System Owner • Chief Information Officer • Authorizing Official or Authorizing Official Designated Representative
TASK P-7 **Continuous Monitoring Strategy—Organization** Develop and implement an organization-wide strategy for continuously monitoring control effectiveness.	• Senior Accountable Official for Risk Management or Risk Executive (Function)	• Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Mission or Business Owner • System Owner • Authorizing Official or Authorizing Official Designated Representative
System Level		
TASK P-8 **Mission or Business Focus** Identify the missions, business functions, and mission/business processes that the system is intended to support.	• Mission or Business Owner	• Authorizing Official or Authorizing Official Designated Representative • System Owner • Information Owner or Steward • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK P-9 **System Stakeholders** Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.	• Mission or Business Owner • System Owner	• Chief Information Officer • Authorizing Official or Authorizing Official Designated Representative • Information Owner or Steward • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Chief Acquisition Officer
TASK P-10 **Asset Identification** Identify assets that require protection.	• System Owner	• Authorizing Official or Authorizing Official Designated Representative • Mission or Business Owner • Information Owner or Steward • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK P-11 **Authorization Boundary** Determine the authorization boundary of the system.	• Authorizing Official	• Chief Information Officer • Mission or Business Owner • System Owner • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Enterprise Architect

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK P-12 **Information Types** Identify the types of information to be processed, stored, and transmitted by the system.	• System Owner • Information Owner or Steward	• System Security Officer • System Privacy Officer • Mission or Business Owner
TASK P-13 **Information Life Cycle** Identify and understand all stages of the information life cycle.	• Senior Agency Official for Privacy • System Owner • Information Owner or Steward	• Chief Information Officer • Mission or Business Owner
TASK P-14 **Risk Assessment—System** Conduct a system-level risk assessment and update the risk assessment on an ongoing basis.	• System Owner • System Privacy Officer	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Authorizing Official or Authorizing Official Designated Representative • Mission or Business Owner • Information Owner or Steward • System Security Officer
TASK P-15 **Requirements** Define the security and privacy requirements for the system and the environment of operation.	• Mission or Business Owner • System Owner • Information Owner or Steward • System Privacy Officer	• Authorizing Official or Authorizing Official Designated Representative • Senior Agency Information Security Officer • Senior Agency Official for Privacy • System Security Officer
TASK P-16 **Enterprise Architecture** Determine the placement of the system within the enterprise architecture.	• Mission or Business Owner • Enterprise Architect • Security Architect • Privacy Architect	• Chief Information Officer • Authorizing Official or Authorizing Official Designated Representative • Senior Agency Information Security Officer • Senior Agency Official for Privacy • System Owner • Information Owner or Steward
TASK P-17 **System Registration** Register the system with organizational program or management offices.	• System Owner	• Mission or Business Owner • Chief Information Officer • System Security Officer • System Privacy Officer

3483

TABLE E-2: CATEGORIZATION TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK C-1 **Security Categorization** Categorize the system and document the security categorization results.	• System Owner • Information Owner or Steward	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Chief Information Officer • Senior Agency Information Security Officer • Authorizing Official or Authorizing Official Designated Representative • System Security Officer • System Privacy Officer
TASK C-2 **Security Categorization Review and Approval** Review and approve the security categorization results and decision.	• Authorizing Official or Authorizing Official Designated Representative • Senior Agency Official for Privacy (for systems processing PII)	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Chief Information Officer • Senior Agency Information Security Officer
TASK C-3 **System Description** Document the characteristics of the system.	• System Owner	• Authorizing Official or Authorizing Official Designated Representative • Information Owner or Steward • System Security Officer • System Privacy Officer

3486 **TABLE E-3: SELECTION TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES**

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK S-1 **Requirements Allocation** Allocate security and privacy requirements to the information system and to the environment of operation.	• Security Architect • Privacy Architect • System Security Officer • System Privacy Officer	• Chief Information Officer • Authorizing Official or Authorizing Official Designated Representative • Mission or Business Owner • Senior Agency Information Security Officer • Senior Agency Official for Privacy • System Owner
TASK S-2 **Control Selection** Select the controls for the system and the environment of operation.	• System Owner • Common Control Provider	• Authorizing Official or Authorizing Official Designated Representative • Information Owner or Steward • Systems Security Engineer • Privacy Engineer • System Security Officer • System Privacy Officer
TASK S-3 **Control Tailoring** Tailor the controls selected for the system and the environment of operation.	• System Owner • Common Control Provider	• Authorizing Official or Authorizing Official Designated Representative • Information Owner or Steward • Systems Security Engineer • Privacy Engineer • System Security Officer • System Privacy Officer
TASK S-4 **Plan Development** Document the controls for the system and environment of operation in security and privacy plans.	• System Owner • Common Control Provider	• Authorizing Official or Authorizing Official Designated Representative • Information Owner or Steward • Systems Security Engineer • Privacy Engineer • System Security Officer • System Privacy Officer
TASK S-5 **Continuous Monitoring Strategy—System** Develop and implement a system-level strategy for monitoring control effectiveness to supplement the organizational continuous monitoring strategy.	• System Owner • Common Control Provider	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Authorizing Official or Authorizing Official Designated Representative • Information Owner or Steward • Security Architect • Privacy Architect • Systems Security Engineer • Privacy Engineer • System Security Officer • System Privacy Officer

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK S-6 **Plan Review and Approval** Review and approve the security and privacy plans for the system and the environment of operation.	• Authorizing Official or Authorizing Official Designated Representative	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Chief Acquisition Officer

3487

3488 **TABLE E-4: IMPLEMENTATION TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES**

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK I-1 **Control Implementation** Implement the controls specified in the security and privacy plans.	• System Owner • Common Control Provider	• Information Owner or Steward • Security Architect • Privacy Architect • Systems Security Engineer • Privacy Engineer • System Security Officer • System Privacy Officer • Enterprise Architect • System Administrator
TASK I-2 **Baseline Configuration** Establish the initial configuration baseline for the system by documenting changes to planned control implementation.	• System Owner • Common Control Provider	• Information Owner or Steward • Security Architect • Privacy Architect • Systems Security Engineer • Privacy Engineer • System Security Officer • System Privacy Officer • Enterprise Architect • System Administrator

3489

3490 TABLE E-5: ASSESSMENT TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK A-1 **Assessor Selection** Select the appropriate assessor or assessment team for the type of control assessment to be conducted.	• Authorizing Official or Authorizing Official Designated Representative	• Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK A-2 **Assessment Plan** Develop, review, and approve plans to assess implemented controls.	• Authorizing Official or Authorizing Official Designated Representative • Control Assessor	• Senior Agency Information Security Officer • Senior Agency Official for Privacy • System Owner • Common Control Provider • Information Owner or Steward • System Security Officer • System Privacy Officer
TASK A-3 **Control Assessments** Assess the controls in accordance with the assessment procedures described in the assessment plans.	• Control Assessor	• Authorizing Official or Authorizing Official Designated Representative • System Owner • Common Control Provider • Information Owner or Steward • Senior Agency Information Security Officer • Senior Agency Official for Privacy • System Security Officer • System Privacy Officer
TASK A-4 **Assessment Reports** Prepare the assessment reports documenting the findings and recommendations from the control assessments.	• Control Assessor	• System Owner • Common Control Provider • System Security Officer • System Privacy Officer
TASK A-5 **Remediation Actions** Conduct initial remediation actions on the controls and reassess remediated controls.	• System Owner • Common Control Provider • Control Assessor	• Authorizing Official or Authorizing Official Designated Representative • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Senior Accountable Official for Risk Management or Risk Executive (Function) • System Owner • Common Control Provider • Information Owner or Steward • Systems Security Engineer • Privacy Engineer • System Security Officer • System Privacy Officer

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK A-6 **Plan of Action and Milestones** Prepare the plan of action and milestones based on the findings and recommendations of the assessment reports.	• System Owner • Common Control Provider	• Information Owner or Steward • System Security Officer • System Privacy Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Chief Acquisition Officer

3491

TABLE E-6: AUTHORIZATION TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK R-1 **Authorization Package** Assemble the authorization package and submit the package to the authorizing official for an authorization decision.	• System Owner • Common Control Provider	• System Security Officer • System Privacy Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Control Assessor
TASK R-2 **Risk Analysis and Determination** Analyze and determine the risk from the operation or use of the system or the provision of common controls.	• Authorizing Official or Authorizing Official Designated Representative	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK R-3 **Risk Response** Identify and implement a preferred course of action in response to the risk determined.	• Authorizing Official or Authorizing Official Designated Representative	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy • System Owner or Common Control Provider • Information Owner or Steward • Systems Security Engineer • Privacy Engineer • System Security Officer • System Privacy Officer
TASK R-4 **Authorization Decision** Determine if the risk from the operation or use of the information system or the provision or use of common controls is acceptable.	• Authorizing Official	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Authorizing Official Designated Representative
TASK R-5 **Authorization Reporting** Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk.	• Authorizing Official or Authorizing Official Designated Representative	• System Owner or Common Control Provider • Information Owner or Steward • System Security Officer • System Privacy Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy

TABLE E-7: MONITORING TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK M-1 **System and Environment Changes** Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system.	• System Owner or Common Control Provider • Senior Agency Information Security Officer • Senior Agency Official for Privacy	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Authorizing Official or Authorizing Official Designated Representative • Information Owner or Steward • System Security Officer • System Privacy Officer
TASK M-2 **Ongoing Assessments** Assess the controls implemented within and inherited by the system in accordance with the continuous monitoring strategy.	• Control Assessor	• Authorizing Official or Authorizing Official Designated Representative • System Owner or Common Control Provider • Information Owner or Steward • System Security Officer • System Privacy Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK M-3 **Ongoing Risk Response** Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones.	• Authorizing Official • System Owner • Common Control Provider	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy; Authorizing Official Designated Representative • Information Owner or Steward • System Security Officer • System Privacy Officer • Systems Security Engineer • Privacy Engineer • Security Architect • Privacy Architect
TASK M-4 **Authorization Updates** Update plans, assessment reports, and plans of action and milestones based on the results of the continuous monitoring process.	• System Owner • Common Control Provider	• Information Owner or Steward • System Security Officer • System Privacy Officer • Senior Agency Official for Privacy • Senior Agency Information Security Officer

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK M-5 **Posture Reporting** Report the security and privacy posture of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy.	• System Owner • Common Control Provider • Senior Agency Information Security Officer • Senior Agency Official for Privacy	• System Security Officer • System Privacy Officer
TASK M-6 **Ongoing Authorization** Review the security and privacy posture of the system on an ongoing basis to determine whether the risk remains acceptable.	• Authorizing Official	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Authorizing Official Designated Representative
TASK M-7 **System Disposal** Implement a system disposal strategy and execute required actions when a system is removed from operation.	• System Owner	• Authorizing Official or Authorizing Official Designated Representative • Information Owner or Steward • System Security Officer • System Privacy Officer • Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy

APPENDIX F

SYSTEM AND COMMON CONTROL AUTHORIZATIONS

AUTHORIZATION DECISIONS AND SUPPORTING EVIDENCE

This appendix provides information on the system and common control authorization processes to include: types of authorizations; content of authorization packages; authorization decisions; authorization decision documents; ongoing authorization; reauthorization; event-driven triggers and significant changes; type and facility authorizations; and authorization approaches.

TYPES OF AUTHORIZATIONS

Authorization is the process by which a senior management official, the *authorizing official*, reviews security- and privacy-related information describing the current security and privacy posture of information systems or common controls that are inherited by systems. The authorizing official uses this information to determine if the mission/business risk of operating a system or providing common controls is acceptable—and if it is, explicitly accepts the risk. Security- and privacy-related information is presented to the authorizing official in an authorization package, which may consist of a report from an automated security/privacy management and reporting tool.[116] System and common control authorization occurs as part of the RMF *Authorize* step. A system authorization or a common control authorization can be an initial authorization, an ongoing authorization, or a reauthorization as defined below:

- *Initial authorization* is defined as the initial (start-up) risk determination and risk acceptance decision based on a complete, zero-based review of the system or of common controls. The zero-based review of the system includes an assessment of all implemented system-level controls (including the system-level portion of the hybrid controls) and a review of the security status of inherited common controls as specified in security and privacy plans.[117] The zero-based review of common controls (other than common controls that are system-based) includes an assessment of applicable controls (e.g., policies, operating procedures, implementation information) that contribute to the provision of a common control or set of common controls.

- *Ongoing authorization* is defined as the subsequent (follow-on) risk determinations and risk acceptance decisions taken at agreed-upon and documented frequencies in accordance with the organization's mission/business requirements and organizational risk tolerance. Ongoing authorization is a time-driven or event-driven authorization process. The authorizing official is provided with the necessary information regarding the near real-time security and privacy posture of the system to determine whether the mission/business risk of continued system

[116] [SP 800-137] provides information on automated security management and reporting tools. Future updates to this publication will also address privacy management and reporting tools.

[117] The zero-based review of a system does not require a zero-based review of the common controls that are available for inheritance by that system. The common controls are authorized under a separate authorization process with a separate authorization official accepting the risk associated with the provision of those controls. The review of the security and privacy plans containing common controls is necessary to understand the current state of the controls being inherited by organizational systems and factoring this information into risk-based decisions associated with the system.

operation or the provision of common controls is acceptable. Ongoing authorization is fundamentally related to the ongoing understanding and ongoing acceptance of security and privacy risk and is dependent on a robust continuous monitoring program.

- *Reauthorization* is defined as the static, single point-in-time risk determination and risk acceptance decision that occurs after initial authorization. In general, reauthorization actions may be time-driven or event-driven. However, under ongoing authorization, reauthorization is in most instances, an event-driven action initiated by the authorizing official or directed by the senior accountable official for risk management or risk executive (function) in response to an event that results in security and privacy risk above the level of risk previously accepted by the authorizing official. Reauthorization consists of a review of the system or the common controls similar to the review carried out during the initial authorization. The reauthorization differs from the initial authorization because the authorizing official can choose to initiate a complete zero-based review of the system or of the common controls or to initiate a targeted review based on the type of event that triggered the reauthorization. Reauthorization is a separate activity from the ongoing authorization process. However, security and privacy information generated from the continuous monitoring program may be leveraged to support reauthorization. The reauthorization actions may necessitate a review of and changes to the organization's information security and privacy continuous monitoring strategies which may in turn affect ongoing authorization.

AUTHORIZATION PACKAGE

The *authorization package* provides a record of the results of the control assessments and provides the authorizing official with the information needed to make a risk-based decision on whether to authorize the operation of a system or common controls.[118] The system owner or common control provider is responsible for the development, compilation, and submission of the authorization package. This includes information available from reports generated by an automated security/privacy management and reporting tool. The system owner or common control provider receives inputs from many sources during the preparation of the authorization package including, for example: senior agency information security officer; senior agency official for privacy, senior accountable official for risk management or risk executive (function); control assessors; system security or privacy officer; and the continuous monitoring program. The authorization package[119] includes the following:

- Executive summary;
- Security and privacy plans;[120]
- Security and privacy assessment reports;[121] and

[118] Authorization packages for common controls that are not system-based may not include a security or privacy plan, but do include a record of common control implementation details.

[119] The authorizing official determines what additional supporting information, artifacts, or references may be required in the authorization package. The additional documentation may include, for example, risk assessments, contingency plans, or SCRM plans.

[120] [SP 800-18] provides guidance on security plans. Guidance on privacy plans will be addressed in future updates to this publication.

[121] [SP 800-53A] provides guidance on security assessment reports. Guidance on privacy assessment reports will be addressed in future updates to this publication.

- Plans of action and milestones.

The executive summary provides a consolidated view of the security and privacy information in the authorization package. The executive summary identifies and highlights risk management issues associated with protecting organizational information systems and the environments in which the systems operate. The summary provides the essential information needed by the authorizing official to understand the security and privacy risks to the organization's operations and assets, individuals, other organizations, and the Nation. This information can be used by the authorizing official to make informed, risk-based decisions regarding the operation and use of the system or the provision of common controls that can be inherited by organizational systems.

The security and privacy plans provide an overview of the security and privacy requirements and describe the controls in place or planned for meeting those requirements. The plans provide sufficient information to understand the intended or actual implementation of the controls implemented within the system and indicate the controls that are implemented via inherited common controls. Additionally, privacy plans describe the methodologies and metrics that will be used to assess the controls. The security and privacy plans may also include as supporting appendices or as references, additional documents such as a privacy impact assessment, interconnection security agreements, security and privacy configurations, contingency plan, configuration management plan, incident response plan, and system-level continuous monitoring strategy. The security and privacy plans are updated whenever events dictate changes to the controls implemented within or inherited by the system.

The security and privacy assessment reports, prepared by the control assessor or generated by automated security/privacy management and reporting tools, provide the findings and results of assessing the implementation of the controls identified in the security and privacy plans to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security and privacy requirements. The assessment reports may contain recommended corrective actions for deficiencies identified in the controls.[122]

Supporting the near real-time risk management objectives of the authorization process, the assessment reports are updated on an ongoing basis whenever changes are made to the controls implemented within or inherited by the system.[123] Updates to the assessment reports help to ensure that system owners, common control providers, and authorizing officials maintain an awareness of control effectiveness. The effectiveness of the controls directly affects the security and privacy posture of the system and decisions regarding explicit acceptance of risk.

The plan of action and milestones, prepared by the system owner or common control provider, describes the specific measures planned to correct deficiencies identified in the controls during

[122] An executive summary provides an authorizing official with an abbreviated version of the security and privacy assessment reports focusing on the highlights of the assessment, synopsis of findings, and recommendations for addressing deficiencies in the security and privacy controls.

[123] Because the desired outcome of ongoing tracking and response to assessment findings to facilitate risk management decisions is the focus (rather than the specific process used), organizations have the flexibility to manage and update security assessment report information using any format or method consistent with internal organizational processes.

the assessment; and to address known vulnerabilities or security and privacy risks.[124] The content and structure of plans of action and milestones are informed by the risk management strategy developed as part of the risk executive (function) and are consistent with the plans of action and milestones process established by the organization which include any specific requirements defined in federal laws, executive orders, policies, directives, or standards. If the systems and the environments in which those systems operate have more vulnerabilities than available resources can realistically address, organizations develop and implement plans of action and milestones that facilitate a prioritized approach to risk mitigation and that is consistent across the organization. This ensures that plans of action and milestones are based on:

- The security categorization of the system and security, privacy, and supply chain risk assessments;
- The specific deficiencies in the controls;
- The criticality of the control deficiencies (i.e., the direct or indirect effect the deficiencies may have on the security and privacy posture of the system and the risk exposure of the organization);[125]
- The risk mitigation approach of the organization to address the identified deficiencies in the controls; and
- The rationale for accepting certain deficiencies in the controls.

Organizational strategies for plans of action and milestones are guided and informed by the security categorization of the systems affected by the risk mitigation activities. Organizations may decide, for example, to allocate their risk mitigation resources initially to the highest-impact systems or other high-value assets because a failure to correct the known deficiencies in those systems or assets could potentially have the most significant adverse effects on their missions or business functions. Organizations prioritize deficiencies using information from risk assessments and the risk management strategy developed as part of the risk executive (function). Therefore, a high-impact system would have a prioritized list of deficiencies for that system, and similarly for moderate-impact and low-impact systems.

AUTHORIZATION DECISIONS

Authorization decisions are based on the content of the authorization package. There are four types of authorization decisions that can be rendered by authorizing officials:

- Authorization to operate;
- Common control authorization;
- Authorization to use; and
- Denial of authorization.

[124] Implementation information about mitigation actions from plans of actions and milestones is documented in the security plan.
[125] In general, risk exposure is the degree to which an organization is threatened by the potential adverse effects on organizational operations and assets, individuals, other organizations, or the Nation.

Authorization to Operate

If the authorizing official, after reviewing the authorization package, determines that the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation is acceptable, an *authorization to operate* is issued for the information system. The system is authorized to operate for a specified period in accordance with the terms and conditions established by the authorizing official. An *authorization termination date* is established by the authorizing official as a condition of the authorization. The authorization termination date can be adjusted at any time by the authorizing official to reflect an increased level of concern regarding the security and privacy posture of the system. For example, the authorizing official may choose to authorize the system to operate only for a short time if it is necessary to test a system in the operational environment before all controls are fully in place, (i.e., the authorization to operate is strictly limited to the time needed to complete the testing objectives).[126] The authorizing official may choose to include operating restrictions such as limiting logical and physical access to a minimum number of users; restricting system use time periods; employing enhanced or increased audit logging, scanning, and monitoring; or restricting system functionality to include only the functions that require live testing. The authorizing official considers results from the assessment of controls that are fully or partially implemented since if the system is ready to be tested in a live environment, many of the controls should already be in place. If the system is under ongoing authorization, a time-driven authorization frequency is specified. Additionally, an adverse event could occur that triggers the need to review the authorization to operate.[127]

Common Control Authorization

A *common control authorization* is similar to an authorization to operate for systems. If the authorizing official, after reviewing the authorization package submitted by the common control provider, determines that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable, a common control authorization is issued. It is the responsibility of common control providers to indicate that the common controls selected by the organization have been implemented, assessed, and authorized and are available for inheritance by organizational systems. Common control providers are also responsible for ensuring that the system owners inheriting the controls have access to appropriate documentation and tools.

Common controls are authorized for a specific time period in accordance with the terms and conditions established by the authorizing official and the organization. An *authorization termination date* is established by the authorizing official as a condition of the initial common control authorization. The termination date can be adjusted at any time to reflect the level of concern by the authorizing official regarding the security and privacy posture of the common controls that are available for inheritance. If the controls are under ongoing authorization, a time-driven authorization frequency is specified. Within any authorization type, an adverse event could occur that triggers the need to review the common control authorization. Common controls that are implemented in a system do not require a separate common control

[126] Formerly referred to as an interim authority to test.

[127] Additional information on event-driven triggers is provided below.

authorization because the controls receive an authorization to operate as part of the system authorization to operate.[128]

Authorization to Use

An *authorization to use* is employed when an organization (hereafter referred to as the customer organization) chooses to accept the information in an existing authorization package produced by another organization (either federal or nonfederal) for an information system that is authorized to operate by a federal entity (referred to as the provider organization).[129] An authorization to use is issued by an authorizing official from the customer organization in lieu of an authorization to operate. The official issuing this type of authorization has the same level of risk management responsibility and authority as an authorizing official issuing an authorization to operate or a common control authorization.[130]

The acceptance of the information in the authorization package from the provider organization is based on a need to use shared systems, services, or applications. A customer organization can issue an authorization to use only after a valid authorization to operate has been issued by another federal entity (i.e., the provider organization).[131] The authorization to operate by the provider organization is a statement of acceptance of risk for the system, service, or application being provided. The authorization to use by the customer organization is a statement of the acceptance of risk in using the system, service, or application with respect to the customer's information. An authorization to use provides opportunities for significant cost savings and avoids a potentially costly and time-consuming authorization process by the customer organization.

An authorization to use requires the customer organization to review the authorization package from the provider organization as the fundamental basis for determining risk.[132] When reviewing the authorization package, the customer organization considers various risk factors such as the time elapsed since the authorization results were produced; the environment of operation (if different from the environment reflected in the authorization package); the impact level of the information to be processed, stored, or transmitted; and the overall risk tolerance of

[128] In certain situations, system owners may choose to inherit controls from other organizational systems that may not be designated officially as common controls. System owners inheriting controls from other than approved common control providers ensure that the systems providing such controls have valid authorizations to operate. The authorizing official of the system inheriting the controls is also made aware of the inheritance.

[129] The term *provider organization* refers to the federal agency or subordinate organization that provides a shared system, service, or application and/or owns and maintains the authorization package (i.e., has granted an Authorization to Operate for the shared system, service, or application). The shared system, service, or application may not be owned by the organization that owns the authorization package, for example, in situations where the shared system, service, or application is provided by an external provider.

[130] Risk-based decisions related to control selection and baseline tailoring actions by organizations providing cloud or shared systems, services, or applications should consider the protection needs of the customer organizations that may be using those cloud or shared systems, services, or applications. Thus, organizations hosting cloud or shared systems, services, or applications should consider the shared risk of operating in those types of environments.

[131] A provisional authorization (to operate) issued by the General Services Administration (GSA) as part of the Federal Risk and Authorization Management Program (FedRAMP) is considered a valid authorization to operate for customer organizations desiring to issue an authorization to use for cloud-based systems, services, or applications.

[132] The sharing of the authorization package (including security and privacy plans, security and privacy assessment reports, plans of action and milestones, and the authorization decision document) is accomplished under terms and conditions agreed upon by all parties (i.e., the customer organization and the service provider organization).

the customer organization. If the customer organization plans to integrate the shared system, application, or service with one or more of its systems, the customer organization considers the risk in doing so.

If the customer organization determines that there is insufficient information in the provider authorization package or inadequate controls in place for establishing an acceptable level of risk, the organization may negotiate with the provider organization and request additional controls or security, privacy, or supply chain information. This may include for example, supplementing controls for risk reduction; implementing compensating controls; conducting additional or more rigorous assessments; or establishing constraints on the use of the system, application, or service provided. The request for additional information may include information the provider organization produced or discovered in the use of the system that is not reflected in the authorization package. When the provider organization does not provide the requested controls, the customer organization may choose to implement additional controls to reduce risk to an acceptable level. The additional controls, along with any other controls for which the customer organization is responsible, are documented, implemented, assessed, authorized, and monitored.

Once the customer organization is satisfied with the security and privacy posture of the shared or cloud system, application, or service (as reflected in the current authorization package) and the risk of using the shared or cloud system, application, or service has been sufficiently mitigated, the customer organization issues an authorization to use in which the customer organization explicitly understands and accepts the security or privacy risk incurred by using the shared system, service, or application.[133] Ultimately, the customer organization is responsible and accountable for the risks that may impact the customer organization's operations and assets, individuals, other organizations, or the Nation.

The authorization to use does not require a termination date, but remains in effect while the customer organization continues to accept the security and privacy risk of using the shared or cloud system, application, or service; and the authorization to operate issued by the provider organization meets the requirements established by federal and organizational policies. It is incumbent on the customer organization to ensure that information from the monitoring activities conducted by the provider organization is shared on an ongoing basis and that the provider organization notifies the customer organization when there are significant changes to the system, application, or service that may affect the security and privacy posture of the provider. If desired, the authorization to use decision may specify time- or even-driven triggers for review of the security and privacy posture of the provider organization system, service, or application being used by the customer organization. The provider organization to notifies the customer organization if there is a significant event that compromises or adversely affects the customer organization's information.

[133] In accordance with [FISMA14], the head of each agency is responsible for providing information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or by a contractor of an agency. [OMB A-130] describes organizational responsibilities for accepting security and privacy risk.

Figure F-1 illustrates the types of authorization decisions that can be applied to organizational systems and common controls and the risk management roles in the authorization process.

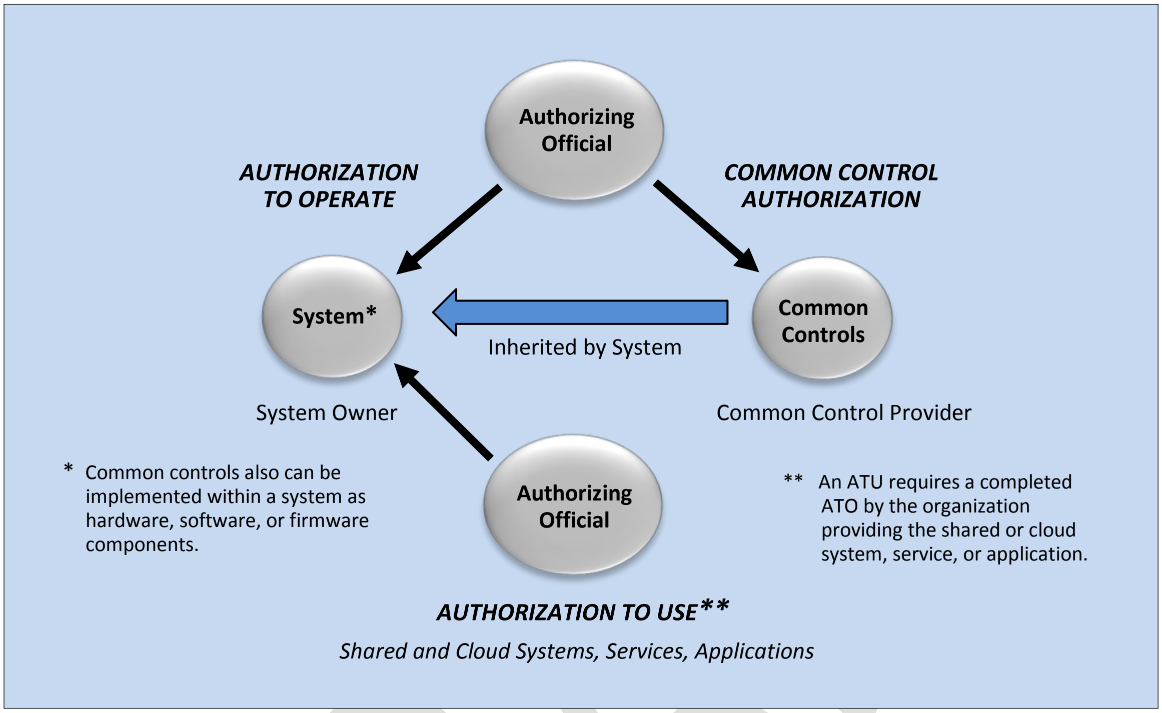

Authorizing Official
AUTHORIZATION TO OPERATE
COMMON CONTROL AUTHORIZATION
System*
Inherited by System
Common Controls
System Owner
Common Control Provider
* Common controls also can be implemented within a system as hardware, software, or firmware components.
Authorizing Official
** An ATU requires a completed ATO by the organization providing the shared or cloud system, service, or application.
AUTHORIZATION TO USE**
Shared and Cloud Systems, Services, Applications

FIGURE F-1: TYPES OF AUTHORIZATION DECISIONS

Denial of Authorization

If the authorizing official, after reviewing the authorization package, including any inputs provided by the senior accountable official for risk management or risk executive (function), determines that the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation is unacceptable and immediate steps cannot be taken to reduce the risk to an acceptable level, the authorization is not granted. A *denial of authorization* means that the information system is not authorized to operate and not placed into operation; common controls are not authorized to be provided to systems; or that the provider's system is not authorized for use by the customer organization. If the system is currently in operation, all activity is halted. Failure to receive an authorization means that there are significant deficiencies in the controls.

The authorizing official or designated representative works with the system owner or the common control provider to revise the plan of action and milestones to help ensure that measures are taken to correct the deficiencies. A special case of authorization denial is an *authorization rescission*. Authorizing officials can rescind a previous authorization decision when there is a violation of federal or organizational policies, directives, regulations, standards, or guidance; or a violation of the terms and conditions of the authorization. For example, failure to maintain an effective continuous monitoring program may be grounds for rescinding an authorization decision.

AUTHORIZATION DECISION INFORMATION

The authorization decision is transmitted from the authorizing official to system owners, common control providers, and other key organizational officials. The authorization decision includes the following information:

- Authorization decision;
- Terms and conditions for the authorization;
- Time-driven authorization frequency or authorization termination date;
- Events that may trigger a review of the authorization decision (if any); and
- For common controls, the [FIPS 199] impact level supported by those controls.

The authorization decision indicates if the system is authorized to operate or authorized to be used; or if the common controls are authorized to be provided to system owners and inherited by organizational systems. The terms and conditions for the authorization provide any limitations or restrictions placed on the operation of the system that must be followed by the system owner or alternatively, limitations or restrictions placed on the implementation of common controls that must be followed by the common control provider. If the system or common controls are not under ongoing authorization, the termination date for the authorization established by the authorizing official indicates when the authorization expires and reauthorization is required. The authorization decision document is transmitted with the original authorization package to the system owner or common control provider.[134]

Upon receipt of the authorization decision and authorization package, the system owner and common control provider acknowledge, implement, and comply with the terms and conditions of the authorization. The system owner and common control provider retain the authorization decision and authorization package.[135] The organization ensures that authorization documents are available to organizational officials when requested. The contents of authorization packages, including sensitive information regarding system vulnerabilities, privacy risks, and control deficiencies, are marked and protected in accordance with federal and organizational policy. Authorization decision information is retained in accordance with the organization's record retention policy. The authorizing official verifies on an ongoing basis, that the terms and conditions established as part of the authorization are being followed by the system owner and common control provider.

Authorization to Use Decision

The authorization to use is a streamlined version of the authorization to operate and includes:

- A risk acceptance statement; and
- Time- or event-driven triggers for review of the security and privacy posture of the provider organization shared cloud or system, application, or service (if any).

[134] Authorization decision documents may be digitally signed to ensure authenticity.

[135] Organizations may choose to employ automated tools to support the development, distribution, and archiving of risk management information to include artifacts associated with the authorization process.

An authorization to use is issued by an authorizing official from a customer organization in lieu of an authorization to operate. The authorizing official has the same level of risk management responsibility and authority as an authorizing official issuing an authorization to operate or a common control authorization. The risk acceptance statement indicates the explicit acceptance of the security and privacy risk incurred from the use of a shared system, service, or application with respect to the customer organization information processed, stored, or transmitted by or through the shared or cloud system, service, or application.

ONGOING AUTHORIZATION

Continuous monitoring strategies[136] promote effective and efficient risk management on an ongoing basis. Risk management can become *near real-time* by using automation and state-of-the-practice tools, techniques, and procedures for the ongoing monitoring of controls and changes to systems and the environments in which those systems operate. Continuous monitoring based on the needs of the authorizing official, produces the necessary information to determine the current security and privacy posture of the system.[137] It also highlights the risks to organizational operations and assets, individuals, other organizations, and the Nation. Ultimately, continuous monitoring guides and informs the authorizing official's decision whether to authorize the continued operation of the system or the continued use of the common controls inherited by organizational systems.

Continuous monitoring helps to achieve a state of *ongoing authorization* where the authorizing official maintains sufficient knowledge of the current security and privacy posture of the system to determine whether continued operation is acceptable based on ongoing risk determinations—and if not, which steps in the RMF need to be revisited to effectively respond to the additional risk. Reauthorizations are unnecessary in situations where the continuous monitoring program provides authorizing officials with the information necessary to manage the risk arising from changes to the system or the environment in which the system operates. If a reauthorization is required, organizations maximize the use of status reports and relevant information about the security and privacy posture of the system that is produced during the continuous monitoring process to improve efficiency.

When a system or common controls are under ongoing authorization, the system or common controls may be authorized on a time-driven and/or event-driven basis, leveraging the security- and privacy-related information generated by the continuous monitoring program. The system and common controls are authorized on a time-driven basis in accordance with the authorization frequency determined as part of the organization- and system-level continuous monitoring strategies. The system and common controls are authorized on an event-driven basis until organizational-defined trigger events occur. Whether the authorization is time-driven or event-driven, the authorizing official acknowledges the ongoing acceptance of identified risks. The organization determines the level of formality required for such acknowledgement by the authorizing official.

[136] [SP 800-137] provides additional guidance on information security continuous monitoring. Guidance on privacy continuous monitoring will be provided in future updates to this publication.

[137] For greater efficiency, the information security continuous monitoring (ISCM) and privacy continuous monitoring (PCM) strategies may be consolidated into a single unified continuous monitoring strategy. Similarly, the ISCM and PCM programs may also be consolidated into a single unified continuous monitoring program.

Conditions for Implementation of Ongoing Authorization

When the RMF has been effectively applied across the organization and the organization has implemented a robust continuous monitoring program, systems may transition from a static, point-in-time authorization process to a dynamic, near real-time ongoing authorization process. To do so, the following conditions must be satisfied:

- The system or common control being considered for ongoing authorization has received an initial authorization based on a complete, zero-based review of the system or the common controls.[138]
- An organizational continuous monitoring program is in place that monitors implemented controls with the appropriate degree of rigor and at the required frequencies specified by the organization in accordance with the continuous monitoring strategy and NIST standards and guidelines.[139]

The organization establishes and implements a process to designate that the two conditions are satisfied and the system or the common controls are transitioning to ongoing authorization. This includes the authorizing official acknowledging that the system or common control are now being managed by an ongoing authorization process and accepting the responsibility for performing all activities associated with that process. The transition to ongoing authorization is documented by the authorizing official by issuing a new authorization decision.[140] The security- and privacy-related information generated through the continuous monitoring process is provided to the authorizing officials and other organizational officials in a timely manner through security and privacy management and reporting tools. Such tools facilitate risk-based decision making for the ongoing authorization for systems and common controls.

Information Generation, Collection, and Independence Requirements

To support ongoing authorization, security- and privacy-related information for controls is generated and collected at the frequency specified in the organization's continuous monitoring strategy. This information may be collected using automated tools or other methods of assessment depending on the type and purpose of the control and desired rigor of the assessment. Automated tools may not generate security- and privacy-related information that is sufficient to support the authorizing official in making risk determinations. This may occur for various reasons, including for example, the tools do not generate information for every control or every part of a control; additional assurance is needed; or the tools do not generate information on specific technologies or platforms. In such cases, manual control assessments are conducted at organizationally-determined frequencies to cover any gaps in automated security- and privacy-related information generation. The manually-generated assessment

[138] System owners and authorizing officials leverage security- and privacy-related information about inherited common controls from assessments conducted by common control providers.

[139] [SP 800-53] and [SP 800-53A] provide guidance regarding the appropriate degree of rigor for security assessments and monitoring. Future updates to Special Publication 800-53A will address privacy assessments.

[140] Prior to transitioning to ongoing authorization, organizations have authorization decision documents that include an authorization termination date. By requiring a new authorization decision document, it is made clear that the system or the common controls are no longer bound to the termination date specified in the initial authorization document because the system and the common controls are now under ongoing authorization.

results are provided to the authorizing official in the manner deemed appropriate by the organization.

To support ongoing authorizations for moderate-impact and high-impact systems, the security- and privacy-related information provided to the authorizing official, whether generated manually or in an automated fashion, is produced and analyzed by an entity that meets the independence requirements established by the organization. The senior agency official for privacy is responsible for assessing privacy controls and for providing privacy-related information to the authorizing official. At the discretion of the organization, privacy controls may be assessed by an independent assessor. The independent assessor is impartial and free from any perceived or actual conflicts of interest regarding the development, implementation, assessment, operation, or management of the organizational systems and common controls being monitored.

Ongoing Authorization Frequency

[SP 800-53] security control CA-6, Part c. specifies that the authorization for a system and any common controls inherited by the system be updated at an organization-established frequency. This reinforces the concept of ongoing authorization. In accordance with CA-6 (along with the security and privacy assessment and monitoring frequency determinations established as part of the continuous monitoring strategy), organizations determine a frequency with which authorizing officials review security- and privacy-related information via the security or privacy management and reporting tool or manual process.[141] This near real-time information is used to determine whether the mission or business risk of operating the system or providing the common controls continues to be acceptable. [SP 800-137] provides criteria for determining assessment and monitoring frequencies.

Under ongoing authorization, *time-driven* authorization triggers refer to the frequency with which the organization determines that authorizing officials are to review security- and privacy-related information and authorize the system (or common controls) for continued operation as described above. Time-driven authorization triggers can be based on a variety of organization-defined factors including, for example, the impact level of the system. When a time-driven trigger occurs, authorizing officials review security- and privacy-related information on the systems for which they are responsible and accountable to determine the ongoing organizational mission or business risk, the acceptability of such risk in accordance with organizational risk tolerance, and whether the approval for continued operation is justified. The organizational continuous monitoring process, supported by the organization's security and privacy management and reporting tools, provides the appropriate functionality to notify the responsible and accountable authorizing official that it is time to review the security- and privacy-related information to support ongoing authorization.

[141] *Ongoing authorization* and *ongoing assessment* are different concepts but closely related. To employ an ongoing authorization approach (which implies an ongoing understanding and acceptance of risk), organizations must have in place, an organization-level and system-level continuous monitoring process to assess implemented controls on an ongoing basis. The findings or results from the continuous monitoring process provides information to authorization officials to support near-real time risk-based decision making.

In contrast to time-driven authorization triggers, *event-driven* triggers necessitate an immediate review of security- and privacy-related information by the authorizing official. Organizations may define event-driven *triggers* (i.e., indicators or prompts that cause an organization to react in a predefined manner) for ongoing authorization and reauthorization. When an event-driven trigger occurs under ongoing authorization, the authorizing official is either notified by organizational personnel (e.g., senior agency information security officer, senior agency official for privacy, system owner, common control provider, or system security or privacy officer) or via automated tools that defined trigger events have occurred requiring an immediate review of the system or the common controls. At any time, the authorizing official may also determine independently that an immediate review is required. This review is conducted in addition to the time-driven frequency review defined in the organizational continuous monitoring strategy and occurs during ongoing authorization when the residual risk remains within the acceptable limits of organizational risk tolerance.[142]

Transitioning from Static Authorization to Ongoing Authorization

The intent of continuous monitoring is to monitor controls at a frequency that is sufficient to provide authorizing officials with the information necessary to make effective, risk-based decisions, whether by automated or manual means.[143] However, if a substantial portion of monitoring is not accomplished via automation, it will not be feasible or practical to move from the current static authorization approach to an effective and efficient ongoing authorization approach. A phased approach for the generation of security- and privacy-related information may be necessary during the transition as automated tools become available and a greater number of controls are monitored by automated techniques. Organizations may begin by generating security- and privacy-related information from automated tools and fill in gaps by generating additional information from manual assessments. As additional automated monitoring functionality is added, processes can be adjusted.

Transitioning from a static authorization process to a dynamic, ongoing authorization process requires considerable thought and planning. One methodology that organizations may consider is to take a phased approach to the migration based on the security categorization of the system. Because risk tolerance levels for low-impact systems are likely to be greater than for moderate-impact or high-impact systems, implementing continuous monitoring and ongoing authorization for low-impact systems first may ease the transition. This allows organizations to incorporate lessons learned as continuous monitoring and ongoing authorization processes are implemented for moderate-impact and high-impact systems. This will facilitate the consistent progression of the continuous monitoring and ongoing authorization implementation from the lowest to the highest impact levels for the systems within the organization. Organizations may also consider employing the phased implementation approach by partitioning their systems into subsystems or system components and subsequently transitioning those subsystems or system components to ongoing authorization one segment at a time until the entire system is ready for

[142] The immediate reviews initiated by specific trigger events may occur simultaneously (i.e., in conjunction) with time-driven monitoring activities based on the monitoring frequencies established by the organization and how the reviews are structured within the organization. The same reporting structure may be used for event- and time-driven reviews to achieve efficiencies.

[143] Privacy continuous monitoring means maintaining ongoing awareness of privacy risks and assessing privacy controls at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.

the full transition (at which time the authorizing official acknowledges that the system is now being managed by an ongoing authorization process).

REAUTHORIZATION

Reauthorization actions occur at the discretion of the authorizing official in accordance with federal or organizational policy.[144] If a reauthorization action is required, organizations maximize the use of security and privacy risk-related information produced as part of the continuous monitoring processes currently in effect. Reauthorization actions, if initiated, can be either time-driven or event-driven. Time-driven reauthorizations occur when the authorization termination date is reached (if one is specified). If the system is under ongoing authorization,[145] a time-driven reauthorization may not be necessary. However, if the continuous monitoring program is not sufficiently comprehensive to fully support ongoing authorization, a maximum authorization period can be specified by the authorizing official. Authorization termination dates are guided and informed by federal and organizational policies and by the requirements of authorizing officials.

Under ongoing authorization, a reauthorization may be necessary if an event occurs that produces risk above the acceptable organizational risk tolerance. This situation may occur, for example, if there was a breach/incident or failure of or significant problems with the continuous monitoring program. Reauthorization actions may necessitate a review of and changes to the continuous monitoring strategy which may in turn, affect ongoing authorization.

For security and privacy assessments associated with reauthorization, organizations leverage security- and privacy-related information generated by the continuous monitoring program and fill in gaps with manual assessments. Organizations may supplement automatically-generated assessment information with manually-generated information in situations where an increased level of assurance is needed. If the security control assessments are conducted by qualified assessors with the necessary independence, use appropriate security standards and guidelines, and are based on the needs of the authorizing official, the assessment results can be applied to the reauthorization.[146]

The senior agency official for privacy is responsible for assessing privacy controls and those assessment results can be cumulatively applied to the reauthorization. Independent assessors may assess privacy controls at the discretion of the organization. The senior agency official for privacy reviews and approves the authorization packages for information systems that process PII prior to the authorizing official making a reauthorization decision. The reauthorization action may be as simple as updating the security and privacy plans, security and privacy assessment reports, and plans of action and milestones—focused only on specific problems or ongoing issues, or as comprehensive as the initial authorization.

[144] Decisions to initiate a formal reauthorization include inputs from the senior agency information security officer, senior agency official for privacy, and senior accountable official for risk management/risk executive (function).

[145] An ongoing authorization approach requires that a continuous monitoring program is in place to monitor all implemented security controls with a frequency specified in the continuous monitoring strategy.

[146] [SP 800-53A] describes the specific conditions when security-related information can be reused to support authorization actions.

The authorizing official signs an updated authorization decision document based on the current risk determination and acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation. In all situations where there is a decision to reauthorize a system or the common controls inherited by organizational systems, the maximum reuse of authorization information is encouraged to minimize the time and expense associated with the reauthorization effort (subject to organizational reuse policy).

EVENT-DRIVEN TRIGGERS AND SIGNIFICANT CHANGES

Organizations define event-driven *triggers* (i.e., indicators or prompts that cause a predefined organizational reaction) for both ongoing authorization and reauthorization. Event-driven triggers may include, but are not limited to:

- New threat, vulnerability, privacy risk, or impact information;
- An increased number of findings or deficiencies from the continuous monitoring program;
- New missions/business requirements;
- Change in the authorizing official;
- Significant change in risk assessment findings;
- Significant changes to the system, common controls, or the environments of operation; or
- Exceeding organizational thresholds.

When there is a change in authorizing officials, the new authorizing official reviews the current authorization decision document, authorization package, any updated documents from ongoing monitoring activities, or a report from automated security/privacy management and reporting tools. If the new authorizing official finds the current risk to be acceptable, the official signs a new or updated authorization decision document, formally transferring responsibility and accountability for the system or the common controls. In doing so, the new authorizing official explicitly accepts the risk to organizational operations and assets, individuals, other organizations, and the Nation. If the new authorizing official finds the current risk to be unacceptable, an authorization action (i.e., ongoing authorization or reauthorization) can be initiated. Alternatively, the new authorizing official may instead establish new terms and conditions for continuing the original authorization, but not extend the original authorization termination date (if not under ongoing authorization).

A significant change is defined as a change that is likely to substantively affect the security or privacy posture of a system. Significant changes to a system that may trigger an event-driven authorization action may include, but are not limited to:

- Installation of a new or upgraded operating system, middleware component, or application;
- Modifications to system ports, protocols, or services;
- Installation of a new or upgraded hardware platform;
- Modifications to how information, including PII, is processed;
- Modifications to cryptographic modules or services; or
- Modifications to security and privacy controls.

Significant changes to the environment of operation that may trigger an event-driven authorization action may include, but are not limited to:

- Moving to a new facility;
- Adding new core missions or business functions;
- Acquiring specific and credible threat information that the organization is being targeted by a threat source; or
- Establishing new/modified laws, directives, policies, or regulations.

The examples of changes listed above are only significant when they represent a change that is likely to affect the security and privacy posture of the system. Organizations establish criteria for what constitutes significant change based on a variety of factors including, for example, mission and business needs; threat and vulnerability information; environments of operation for systems; privacy risks; and security categorization.

Risk assessment results or the results from an impact analysis may be used to determine if changes to systems or common controls are significant and trigger an authorization action. If an authorization action is initiated, the organization targets only the specific controls affected by the changes and reuses previous assessment results wherever possible. An effective monitoring program can significantly reduce the overall cost and level of effort of authorization actions. Most changes to a system or its environment of operation can be handled through the continuous monitoring program and ongoing authorization.

TYPE AND FACILITY AUTHORIZATIONS

A *type authorization*[147] is an official authorization decision that allows for a single authorization package to be developed for an archetype (i.e., common) version of a system. This includes, for example hardware, software, or firmware components that are deployed to multiple locations for use in specified environments of operation (e.g., installation and configuration requirements or operational security and privacy needs provided by the host organization at a specific location). A type authorization is appropriate when the system is deployed in a defined environment and is comprised of identical instances of system architecture, software, identical information types, functionally identical hardware, information that is processed in the same way, identical control implementations, or identical configurations. A type authorization is used in conjunction with authorized site-specific controls[148] or with a facility authorization as described below. A type authorization is issued by the authorizing official responsible for the development of the system[149] and represents an authorization to operate. At the site or facility where the system is deployed, the authorizing official who is responsible for the system at the

[147] Examples of type authorizations include: an authorization of the hardware and software applications for a standard financial system deployed in multiple locations; or an authorization of a common workstation or operating environment (i.e., hardware, operating system, and applications) deployed to all operating units within an organization.

[148] Site-specific controls are typically implemented by an organization as *common controls*. Examples include physical and environmental protection controls and personnel security controls.

[149] Typically, type authorizations are issued by organizations that are responsible for developing standardized hardware and software capabilities for customers and delivered to the recipient organizations as “turn key” solutions. The senior leaders issuing such authorizations may be referred to as developmental authorizing officials.

site or facility accepts the risk of deploying the system and issues an authorization to use. The authorization to use leverages the information in the authorization packages for the archetype system and the facility common controls.

A *facility authorization* is an official authorization decision that is focused on specific controls implemented in a defined environment of operation to support one or more systems residing within that environment. This form of authorization addresses common controls within a facility and allows systems residing in the defined environment to inherit the common controls and the affected system security and privacy plans to reference the authorization package for the facility. The common controls are provided at a specified impact level to facilitate risk decisions on whether it is appropriate to locate a given system in the facility.[150] Physical and environmental controls are addressed in a facility authorization but other controls may also be included, for example, boundary protections; contingency plan and incident response plan for the facility; or training and awareness and personnel screening for facility staff. The facility authorizing official issues a common control authorization to describe the common controls available for inheritance by systems residing within the facility.

TRADITIONAL AND JOINT AUTHORIZATIONS

Organizations can choose from two distinct approaches when planning for and conducting authorizations. These include an authorization with a *single* authorizing official or an authorization with *multiple* authorizing officials.[151] The first approach is the traditional authorization process defined in this appendix where a single organizational official in a senior leadership position is responsible and accountable for a system or for common controls. The organizational official accepts the security- and privacy-related risks that may adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation.

The second approach, *joint authorization*, is employed when multiple organizational officials either from the same organization or different organizations, have a shared interest in authorizing a system. The organizational officials collectively are responsible and accountable for the system and jointly accept the security- and privacy-related risks that may adversely impact organizational operations and assets, individuals, other organizations, and the Nation. A similar authorization process is followed as in the single authorization official approach with the essential difference being the addition of multiple authorizing officials. Organizations choosing a joint authorization approach are expected to work together on the planning and the execution of RMF tasks and to document their agreement and progress in implementing the tasks.

Collaboration on security categorization, control selection and tailoring, a plan for assessing controls to determine effectiveness, a plan of action and milestones, and a system-level continuous monitoring strategy is necessary for a successful joint authorization. The terms and conditions of the joint authorization are established by the participating parties in the joint authorization including, for example, the process for ongoing determination and acceptance of risk. The joint authorization remains in effect only while there is agreement among authorizing officials and the authorization meets the specific requirements established by federal and

[150] For example, if the facility is categorized as moderate impact, it may not be appropriate to locate high-impact systems or system components in that environment of operation.

[151] Authorization approaches can be applied to systems and to common controls inherited by organizational systems.

organizational policies. [SP 800-53] controls CA-6 (1), *Joint Authorization – Same Organization* and CA-6 (2) *Joint Authorization – Different Organizations*, describe the requirements for joint authorizations.

APPENDIX G

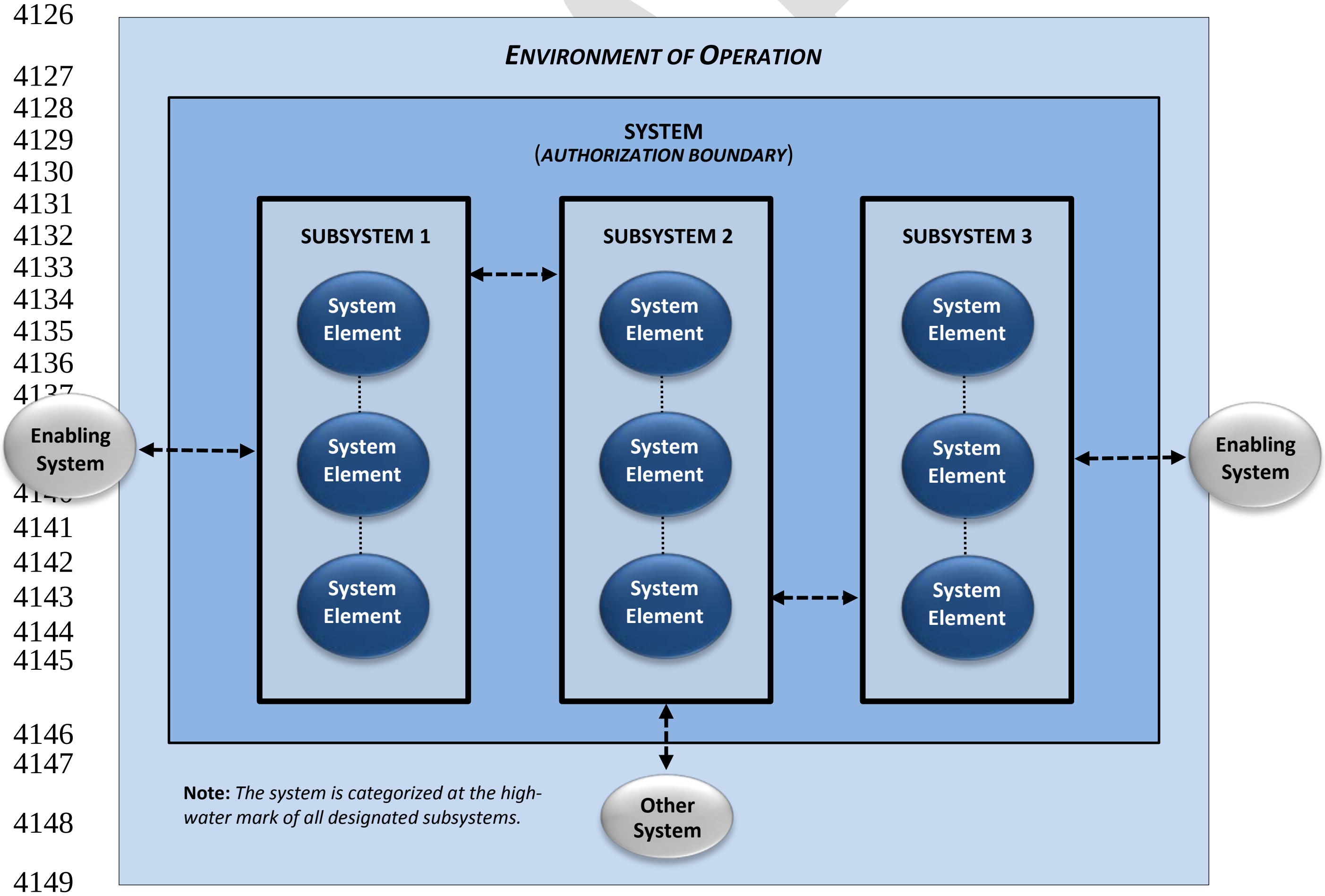
AUTHORIZATION BOUNDARY CONSIDERATIONS

COMPLEX SYSTEMS, APPLICATIONS, AND THE EFFECTS OF CHANGING TECHNOLOGIES

This appendix provides additional considerations for determining authorization boundaries for complex systems and software applications. It also includes guidance on authorization boundaries when organizations use external providers for their information resources. The foundational RMF steps and tasks described in Chapter Three can be applied in all three scenarios to help organizations manage security and privacy risks and comply with the laws, executive orders, and OMB policies discussed in Chapter One.

AUTHORIZATION BOUNDARIES FOR COMPLEX SYSTEMS

The determination of authorization boundaries for complex systems can present significant challenges to organizations. A complex system can be viewed as set of individual subsystems. A subsystem is a major subdivision of a system consisting of system elements that perform one or more specific functions. Figure G-1 illustrates the concept of a complex system.



Note: *The system is categorized at the high-water mark of all designated subsystems.*

FIGURE G-1: CONCEPTUAL VIEW OF A COMPLEX SYSTEM

Organizations can employ the concept of subsystems to divide complex systems into a set of manageable components or identify those components that support a similar in mission, but are sufficiently distinct to be identified separately. Each subsystem has its own boundary (distinct from an authorization boundary) and can be defined within a comprehensive authorization boundary that includes all subsystems.

For example, an organization may find it useful to combine several systems that are under the same direct management control or that have similar missions or business functions into a single system to achieve the dual purposes of effective risk and resource management. An organization may also choose to develop a system composed of multiple independent systems (distributed across a widespread geographic area) supporting a set of common missions or business functions. Similarly, a system can be divided into multiple subsystems to facilitate and support management of the system and risk-based decision making (e.g., categorization decisions, tailoring decisions, and control allocation decisions).

Dividing a system into subsystems (i.e., divide and conquer) facilitates a targeted application of controls to achieve adequate security, protection of individual privacy, and a cost-effective risk management process. Dividing complex systems into subsystems also supports the important security concepts of domain separation and network segmentation, which can be significant when dealing with high-value assets.

Information security and privacy architectures play a key part in the process of dividing complex systems into subsystems. This includes monitoring and controlling communications at internal boundaries among subsystems and selecting, allocating, and implementing controls that meet or exceed the security and privacy requirements of the constituent subsystems. One approach to control selection and allocation is to categorize each identified subsystem separately (see Task C-1). However, separately categorizing each subsystem does not change the overall categorization of the system. Rather, it allows the subsystems to receive a separate and more targeted allocation of controls from [SP 800-53] instead of deploying higher-impact controls across the entire system (see Task S-1). Another approach is to bundle smaller subsystems into larger subsystems within the complex system, categorize each of the aggregated subsystems, and allocate controls to the subsystems, as needed. While subsystems within complex systems may exist as complete systems, the subsystems are, in most cases, not treated as independent entities because they are typically interdependent and interconnected.

When the security categorizations for the identified subsystems are different (e.g., low-impact versus high-impact), the organization examines the subsystem interfaces, information flows, and security- and privacy-related dependencies among subsystems and selects the appropriate controls for the interconnection of the subsystems to eliminate/reduce potential vulnerabilities. This helps to ensure that the system is adequately protected.[152] Controls for the interconnection of subsystems are also employed when the subsystems implement different security and privacy

[152] The types of interfaces and couplings among subsystems may introduce inadvertent vulnerabilities in a complex system. For example, if a large organizational intranet is decomposed into smaller subsystems (e.g., severable systems such as local area network segments) and subsequently categorized individually, the specific protections at the system level may expose an attack vector against the intranet by erroneously selecting and implementing controls that are not sufficiently strong with respect to the rest of the system. To avoid this situation, organizations carefully examine the interfaces among subsystems and take appropriate actions to eliminate potential vulnerabilities in this area, thus helping to ensure that the information system is adequately protected.

policies or are administered by different authorities. The extent to which the selected controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the complex system, can be determined by combining control assessments at the system level and adding considerations addressing interface issues. This approach facilitates a more targeted and cost-effective risk management process by scaling the level of effort of the assessment in accordance with the system categorization and allowing for reuse of assessment results at the system level.

AUTHORIZATION BOUNDARIES FOR SOFTWARE APPLICATIONS

Authorization boundaries include all system components, including hardware, firmware, and software. Software components include applications (e.g., database applications, customized business applications, and web applications), middleware, and operating systems. The software components are included in authorization boundaries, either as part of the information system on which the software is hosted or as a part of an application-only system or subsystem that inherits controls from the hosting system. Software applications may depend on the resources provided by the hosting system and as such, can leverage the controls provided by the hosting system to help provide a foundational level of protection for the hosted applications. Additional application-level controls are provided by the respective software applications, as needed. Application owners coordinate with system owners to help ensure that security and privacy requirements are satisfied among applications and hosting systems. This coordination includes, for example, consideration for the selection, implementation, assessment, and monitoring of controls for the applications; the effects of changes to the applications on the security and privacy posture of the system and the organization; and the effects of changes to the system on the hosted applications.

AUTHORIZATION BOUNDARIES AND EXTERNAL PROVIDERS

While the concepts of external systems and external service providers are not new, the current pervasiveness and frequency of their invocation can present organizations with significant, new challenges. There are instances where system components, subsystems, or perhaps the entire system may be outside of the direct control of the organization that authorizes its operation. The nature of such external systems can vary from organizations employing external cloud computing services to process, store, and transmit federal information to organizations allowing platforms under their control to host applications or services developed by some external entity.[153]

FISMA and OMB policy require external providers that process, store, or transmit federal information or operate information systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies. Federal security and privacy requirements also apply to external systems storing, processing, or transmitting federal information and any services provided by or associated with the external system. Furthermore, the assurance or confidence that the risk from using external providers is at an acceptable level depends on the trust that the organization places in the provider. In some instances, the level of trust is based on the amount of direct control the organization can exert on the provider

[153] The Federal Risk and Authorization Management Program (FedRAMP) operated by the General Services Administration (GSA) provides guidance on determining cloud authorization boundaries.

regarding the employment of controls necessary to protect federal information and protect the privacy of individuals.

The level of trust can also be based on the evidence brought forth by the external provider or by an independent assessor as to the effectiveness of those controls. In other instances, trust can be based on other factors, such as the previous experience the organization has had with the external provider and the confidence the organization has in the provider taking the correct actions. There are a variety of factors that can complicate the level of trust with external providers:

- The delineation between what is owned by the external provider and the organization may be blurred (e.g., organization-owned platform executing external provider-developed application, software module, or firmware);
- The degree of control the organization has over the external provider may be very limited;
- The nature and content of the system, subsystem, service, or application may be subject to rapid change; and
- The system, subsystem, service, or application may be of such critical nature that it needs to be incorporated into organizational systems very rapidly.

The consequence of the above factors is that some of the traditional means organizations use to verify and validate the correct functioning of a system, subsystem, application or service and the effectiveness of implemented controls (e.g., clearly defined requirements, design analysis, testing and evaluation before deployment, control assessments and continuous monitoring) may not be feasible. As a result, organizations may be left to depend upon the nature of the trust relationships with the external provider as the basis for determining whether to issue an authorization to use or authorization to operate for the system or subsystems processing, storing, or transmitting federal information (e.g., use of GSA list of approved providers). Alternatively, organizations may allow externally provided systems or services to be used only in those instances where the exchange of information risk determined by the organization is acceptable.

Ultimately, when the level of trust in the external provider does not provide sufficient assurance, the organization employs compensating controls; accepts greater risk; contracts with a more trustworthy external provider; or does not obtain the service (i.e., conducts its missions and business operations with reduced levels of functionality or possibly no functionality at all).

LEVERAGING EXTERNAL PROVIDER CONTROLS AND ASSESSMENTS

Organizations should exercise caution when attempting to leverage external provider controls and assessment results. Controls implemented by external providers may be different than the controls in [SP 800-53] in the scope, coverage, and capability provided. NIST provides a mapping of the controls in its catalog to the [ISO 27001] security controls and to the [ISO 15408-2] and [ISO 15408-3] security requirements. However, such mappings are inherently subjective and should be reviewed carefully by organizations to determine if the controls and requirements addressed by external providers meet the protection needs of the organization.

Similar caution should be exercised when attempting to use or leverage security and privacy assessment results from external providers. The type, rigor, and scope of the assessments may vary widely from provider to provider. In addition, the assessment procedures employed by the provider and the independence of the assessors conducting the assessments are critical issues that should be reviewed and considered by organizations prior to leveraging assessment results.

Effective risk decisions by authorizing officials depend on the transparency of controls selected and implemented by external providers and the quality and efficacy of the assessment evidence produced by those providers. Transparency is essential to achieve the assurance necessary to ensure adequate protection for organizational assets.

APPENDIX H

SYSTEM LIFE CYCLE CONSIDERATIONS

OTHER FACTORS EFFECTING THE EXECUTION OF THE RMF

All systems, including operational systems, systems under development, and systems that are undergoing modification or upgrade, are in some phase of the SDLC.[154] Defining requirements is a critical part of an SDLC process and begins in the *initiation* phase.[155] Security and privacy requirements are part of the functional and nonfunctional[156] requirements allocated to a system. The security and privacy requirements are incorporated into the SDLC simultaneously with the other requirements. Without the early integration of security and privacy requirements, significant expense may be incurred by the organization later in the life cycle to address security and privacy concerns that could have been included in the initial design. When security and privacy requirements are defined early in the SDLC and integrated with other system requirements, the resulting system has fewer deficiencies, and therefore, fewer privacy risks or security vulnerabilities that can be exploited in the future.

Integrating security and privacy requirements into the SDLC is the most effective, efficient, and cost-effective method to ensure that the organization's protection strategy is implemented. It also ensures that security- and privacy-related processes are not isolated from the other processes used by the organization to develop, implement, operate, and maintain the systems supporting ongoing missions and business functions. In addition to incorporating security and privacy requirements into the SDLC, the requirements are integrated into the organization's program, planning, and budgeting activities to help ensure that resources are available when needed and program and project milestones are completed. The enterprise architecture provides a central record of this integration within an organization.

RISK MANAGEMENT IN THE SYSTEM DEVELOPMENT LIFE CYCLE

Risk management activities begin early in the SDLC and continue throughout the life cycle. These activities are important in helping to shape the security and privacy capabilities of the system; ensuring that the necessary controls are implemented and that the security and privacy risks are being adequately addressed on an ongoing basis; and ensuring that the authorizing officials understand the current security and privacy posture of the system in order to accept the risk to organizational operations and assets, individuals, other organizations, and the Nation.

Ensuring that security and privacy requirements are integrated into the SDLC helps facilitate the development and implementation of more resilient systems to reduce the security and privacy risk to organizational operations and assets, individuals, other organizations, and the Nation.

[154] There are five phases in the SDLC including initiation; development and acquisition; implementation; operation and maintenance; and disposal. [SP 800-64] provides guidance on the SDLC.

[155] Organizations may employ a variety of development processes including, for example, waterfall, spiral, or agile.

[156] Nonfunctional requirements include, for example, quality and assurance requirements.

This can be accomplished by using the concept of integrated project teams.[157] Organizational officials ensure that security and privacy professionals are part of the SDLC activities. Such consideration fosters an increased level of cooperation among personnel responsible for the development, implementation, assessment, operation, maintenance, and disposition of systems and the security and privacy professionals advising the senior leadership on the controls needed to adequately mitigate security and privacy risks and protect organizational missions and business functions.

Finally, organizations maximize the use of security- and privacy-relevant information generated during the SDLC process to satisfy requirements for similar information needed for other security and privacy purposes. The reuse of such information is an effective method to reduce or eliminate duplication of effort, reduce documentation, promote reciprocity, and avoid unnecessary costs that may result when security and privacy activities are conducted independently of the SDLC processes. Reuse promotes consistency of information used in the development, implementation, assessment, operation, maintenance, and disposition of systems including security- and privacy-related considerations.

[157] Integrated project teams are multidisciplinary entities consisting of individuals with a range of skills and roles to help facilitate the development of systems that meet the requirements of the organization.

THE IMPORTANCE OF ARCHITECTURE AND ENGINEERING

Security architects, privacy architects, systems security engineers, and privacy engineers can play an essential role in the SDLC and in the successful execution of the RMF. These individuals provide *system owners* and *authorizing officials* with technical advice on the selection and implementation of controls in organizational information systems—guiding and informing risk-based decisions across the enterprise.

Security and Privacy Architects:

- Ensure that security and privacy requirements necessary to protect mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the systems supporting those missions and business processes.
- Serve as the primary liaison between the enterprise architect and the systems security and privacy engineers.
- Coordinate with system owners, common control providers, and system security and privacy officers on the allocation of controls.
- Advise authorizing officials, chief information officers, senior accountable officials for risk management/risk executive (function), senior agency information security officers, and senior agency officials for privacy on a range of security and privacy issues.

Security and Privacy Engineers:

- Ensure that security and privacy requirements are integrated into systems and system components through purposeful security or privacy architecting, design, development, and configuration.
- Employ best practices when implementing controls within a system, including the use of software engineering methodologies; systems security or privacy engineering principles; secure or privacy-enhancing design, secure or privacy-enhancing architecture, and secure or privacy-enhancing coding techniques.
- Coordinate security- and privacy-related activities with senior agency information security officers, senior agency officials for privacy, security and privacy architects, system owners, common control providers, and system security or privacy officers.